

Using Symantec AntiVirus for Macintosh®



Symantec AntiVirus for Macintosh®

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Copyright Notice

Copyright © 1992-1997 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make change without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, Peter Norton Group, 10201 Torre Avenue, Cupertino, CA 95014.

Trademarks

Symantec, Norton Utilities, Norton Disk Doctor, SAM (Symantec AntiVirus for Macintosh), Speed Disk, THINK C, and THINK Pascal are trademarks of Symantec Corporation.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2

Credits

Software Development

Stuart Davison, Steve Forgacs, Lee Gummerman, Mitch Jones, Scott Roberts

Product Management

Lily Duong, Mary Engstrom, Vicki Routs

Quality Assurance

Matt Candeleria, Michael Emfinger, Herb Hrowal

Documentation and Online Help

Cindy Abernethy, Elizabeth Anders, Annette Brown, Alfred Ghadimi, Karen Goldsmith, Robert Hoffman, Sheelagh O'Connor, Laura Weatherford, Denise Weatherwax

Technical Support

John Bazile, Thomas Borloglou-Boyd, Gregory Freeman, Ted Flug, Brian Huberd, Braden Kelley, Steve Northcutt, Paul Rybicki, Henry W. Schaup, Steve Wolf, Stephen Zeffren

Engineering Services

Alena Cespivova, Richard Espy, Kirsten Hill, Will Jobe, Kim Johnston

Symantec AntiVirus Research Center (SARC)

Frank Barajas, Gioconda Becerra, Chris Brown, Sherralee Buzzell, Matt Candeleria, Shane Coursen, Philip DeBats, Chris Formulak, Alex Haddox, Kevin Marcus, Linh Nguyen, Abid Oonwala, Charles Renert, David Shannon, Jeffrey Sulton, John Wilber

NOW THAT YOU'VE ACCESSED THE WORLD'S BEST SOFTWARE, WHY NOT ACCESS THE WORLD?

**FREE
INTRODUCTORY
OFFER ON
COMPUERVE**

CompuServe® is the most powerful online service available, offering a wide variety of services and forums to over 1,000,000 active members worldwide. You can be a part of it with Symantec's Free Introductory Membership offer. All you need is a personal computer, telecommunications software, and a modem, and you can take advantage of all these powerful features:

ONLINE COMPUTER SUPPORT

ELECTRONIC BROKERAGE SERVICES

ELECTRONIC MAIL AND FAX

ONLINE INTERACTION WITH THOUSANDS OF OTHER USERS

ACCESS TO HUNDREDS OF DATABASES

One more powerful reason
to take advantage of this free offer...

THE SYMANTEC FORUM

GET ONLINE WITH SYMANTEC™ AND COMPUERVE.

Now, there's a powerful, new channel of communication between Symantec and our customers. It's the Symantec Forum on the CompuServe Information Service, and it's a great way to stay on top of the latest information and ideas from Symantec.

The Symantec Forum is our way of making sure you get the most out of your Symantec software. Whether you're a novice user or an expert, we want to answer your questions, hear your suggestions, and know what you're thinking about your Symantec products.

SYMANTEC REPRESENTATIVES AND USERS ARE AS CLOSE AS YOUR KEYBOARD.

With the Symantec Forum, you can interact with Symantec customer service representatives, who are available to answer your questions about any of our products.

It's never been so easy to get answers to your questions and share information with other users.

What's more, the Symantec Forum gives you valuable, up-to-the-minute information, such as:

- Technical Bulletins
- Trial Offers and Demo Software
- Product Add-Ons
- New Symantec Products
- Upgrade Information
- Sample Code
- Tips and Shortcuts
- Training Workshop Dates

IT'S FOR SYMANTEC CUSTOMERS ONLY, AND IT'S ABSOLUTELY FREE!

If you are already a CompuServe member, simply enter GO SYMANTEC at any prompt to enter the Symantec Forum. This free offer is limited to first-time subscribers only. One per customer. Original reply cards only, please; copies will not be accepted.

YES!

I WANT TO GET ONLINE WITH SYMANTEC.

Become a member of CompuServe today, and be a part of the Symantec Forum.
Complete, cut out, place in an envelope, and mail the coupon to the address below and you'll receive:

- A PRIVATE USER ID NUMBER AND PASSWORD
- \$15.00 INTRODUCTORY USAGE CREDIT
- A COMPLEMENTARY SUBSCRIPTION TO *COMPUSERVE MAGAZINE*, COMPUSERVE'S MONTHLY COMPUTING MAGAZINE

**TO GET ONLINE EVEN FASTER, CALL TOLL-FREE 1-800-848-8199 AND ASK FOR
REPRESENTATIVE #124. OUTSIDE THE U.S. AND CANADA, CALL 1-614-457-0802.**

United States and Canada
CompuServe Information Services

Department 124

P.O. Box 20212

Columbus, OH 48220-9988

Telephone: 1-800-848-8199, ask for representative #124

Mexico

(+52) (5) 629-8190



FREE INTRODUCTORY COMPUSERVE RESPONSE CARD — MAIL IN TODAY!

Name _____

Address _____

City _____ State _____

Country _____ Zip/Postal Code _____

Phone _____

SYMANTEC.TM

SYMANTEC LICENSE AND WARRANTY

The software which accompanies this license (the "Software") is the property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, you will have certain rights to use the Software after your acceptance of this license. Except as may be modified by a license addendum which accompanies this license, your rights and obligations with respect to the use of this Software are as follows:

- You may:

- (i) use one copy of the Software on a single computer;
- (ii) make one copy of the Software for archival purposes, or copy the software onto the hard disk of your computer and retain the original for archival purposes;
- (iii) use the Software on a network, provided that you have a licensed copy of the Software for each computer that can access the Software over that network;
- (iv) after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software and the transferee agrees to the terms of this agreement; and
- (v) if a single person uses the computer on which the Software is installed at least 80% of the time, then after returning the completed product registration card which accompanies the Software, that person may also use the Software on a single home computer.

- You may not:

- (i) copy the documentation which accompanies the Software;
- (ii) sublicense, rent or lease any portion of the Software;
- (iii) reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software; or
- (iv) use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version as a replacement of the prior version, unless you donate a previous version of an upgraded version to a charity of your choice, and such charity agrees in writing that it will be the sole end user of the product, and that it will abide by the terms of this agreement. Unless you so donate a previous version of an upgraded version, upon upgrading the Software, all copies of the prior version must be destroyed.

- Sixty Day Money Back Guarantee:

If you are the original licensee of this copy of the Software and are dissatisfied with it for any reason, you may return the complete product, together with your receipt, to Symantec or an authorized dealer, postage prepaid, for a full refund at any time during the sixty day period following the delivery to you of the Software.

- Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money you paid for the Software. Symantec does not warrant that the Software will meet your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

- Disclaimer of Damages:

REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

- U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c) (1) and (2) of the Commercial Computer Software-Restricted Rights clause at 48 CFR 52.227-19, as applicable, Symantec Corporation, 10201 Torre Avenue, Cupertino, CA 95014.

- General:

This Agreement will be governed by the laws of the State of California. This Agreement may only be modified by a license addendum which accompanies this license or by a written document which has been signed by both you and Symantec. Should you have any questions concerning this Agreement, or if you desire to contact Symantec for any reason, please write:

Symantec Customer Service, 175 W. Broadway,
Eugene, OR 97401.

SYMANTEC SOFTWARE LICENSE ADDENDUM

Symantec Software License Addendum

Notwithstanding any of the terms and conditions contained in the Symantec Software License, you may make and use up to that number of copies of the Software that is indicated on the License Authorization Coupon contained in your box. The coupon will constitute proof of your right to make and use such additional copies.

Dual Media Software

If the Software package contains both 3.5" and 5.25" disks, then you may use only the disks appropriate for your computer. You may not use the other disks on another computer or provide them to another user except as part of the permanent transfer (as provided above) of the Software.

Contents

Chapter 1 Installing SAM

System Requirements	17
Performing an Easy Install	17
Performing a Custom Install	19
Where to Go After Installation	21

Chapter 2 Getting Started

Answers to Virus Questions	24
Starting and Exiting SAM	26
Turning SAM Intercept Off and On	27
Getting Help	28
Using Balloon Help	30

Chapter 3 Checking for Viruses

Scanning Disks	31
Scanning Folders and Files	33
Scanning Multiple Floppy Disks	35
Working with Scan Results	36
Printing a Scan Report	37
Saving a Scan Report to a File	37

Chapter 4 Taking Corrective Action

What to Do Next	39
Responding to Virus Alerts	39
Eliminating Viruses	40
Deleting versus Repairing	41
Deleting Infected Files	41
Repairing Infected Files	42
Repairing Multiple Floppy Disks	43
What to Do if Repair Is Unsuccessful	44
Resolving File Irregularities	44
Viewing File Details	46
Responding to Suspicious Activity Alerts	47
Responding to File Changed Alerts	48

Chapter 5 Taking Precautions Against Viruses

Avoiding Viruses	51
Scheduling Events	52
Scheduling Virus Scans	52
Scheduling Virus Definition Updates	54
Editing Scheduled Events	55
Deleting Scheduled Events	55
Protecting Against Unknown Viruses	56
Monitoring for Suspicious Activities	56
Creating a Decontamination Disk	59

Chapter 6 Keeping Up with New Viruses

About the Virus Definitions Files	63
Viewing the Virus List	63
Viewing Virus Descriptions	64
Adding New Virus Definitions	66
Updating Virus Definitions Automatically	66
Updating Virus Definitions from a BBS	70
Updating Virus Definitions from the Internet	71
Updating Virus Definitions from Disk	71
Adding Virus Definitions Manually	72
Deleting Virus Definitions	75
Transferring Virus Definitions to Other Disks	76

Chapter 7 Customizing SAM

Customizing Startup Options	77
Customizing Floppy Disk Scanning	78
Customizing Suspicious Activity Monitoring	80
Customizing Scanning Options	83
Customizing Alerts	85
Customizing Reporting Options	88
Customizing Scan Reports	88
Customizing the Activity Log	89
Defining Hot Keys for Scanning	90
Modifying Hot Keys	92
Deleting Hot Keys	92
Selecting File Compression Options	93
Specifying SafeZones	94
Password-Protecting SAM	95
Changing Your Password	97
Removing Password Protection	97

Chapter 8 Menu Reference

File Menu	99
Edit Menu	100
Tools Menu	101
Preferences Menu	103

Appendix A About Computer Viruses

What Are Computer Viruses?	107
What Viruses Do	107
What Viruses Don't Do	108
How Viruses Spread	108
About Trojan Horses	109
About Worms	109
Getting More Information	109

Appendix B Decontamination Procedures

Appendix C Troubleshooting

General Macintosh Troubleshooting	117
Other Steps to Take	119

Appendix D System Messages

Appendix E Using SAM on a Network

Notes to the Administrator	133
Scanning Network Drives	133
Using SAM Intercept on a Server	134
Preparing an Emergency Response Plan	134
Before a Virus Is Detected	135
If a Virus is Detected	136

Glossary

Symantec Service and Support Solutions

Disk Exchange and/or Replacement Form

Index

How to Use This Manual

This manual describes SAM features and gives procedures for using them.

All instructions in this manual assume that you are familiar with basic Macintosh operations, such as clicking and dragging the mouse; selecting, copying, and moving icons; choosing commands from pull-down and pop-up menus; managing windows; and using the Finder, Chooser, and Control Panels. If you are not familiar with these terms and operations, read your Macintosh user's guide to learn more about operating your Macintosh.

To help you find information, this manual adheres to the following conventions:



Indicates a warning. Read it carefully.

Italics

Indicates a glossary term, or emphasizes a given word.

SMALL CAPS

Indicates the name of a pull-down menu command.

Initial Caps

Indicates the name of an object, such as a menu, a dialog box, or a dialog box component.

boldface

Indicates an option in a dialog box, including pop-up menu options.

Installing SAM

1

This chapter explains how to install SAM on your computer's hard disk and outlines what you should and can do after installation is complete.

System Requirements

In order to run SAM, your system must include:

- Macintosh Plus or later
- System 7.0 or higher
- 2MB or more of RAM
- 2MB of disk space

NOTE: If your Macintosh has low density floppy drives, you must exchange the disks in your SAM package for low density disks. See the “[Disk Exchange and/or Replacement Form,](#)” at the back of this manual.

Performing an Easy Install

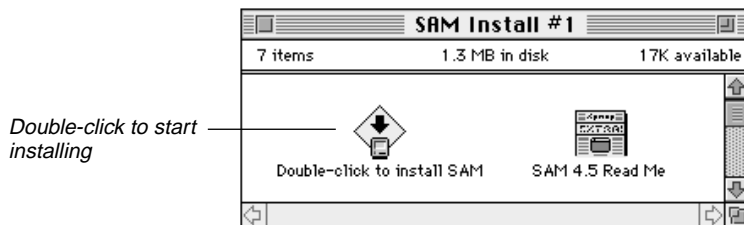
Use the SAM installer located on the SAM Install #1 disk to install the SAM files to your hard disk.

To install SAM:

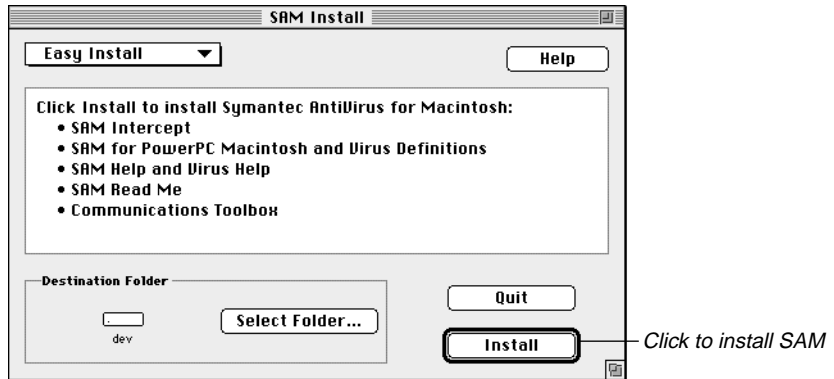
- 1 Insert the SAM Install #1 disk into your floppy drive.

A window displaying the disk contents opens automatically (Figure 1-1).

Figure 1-1



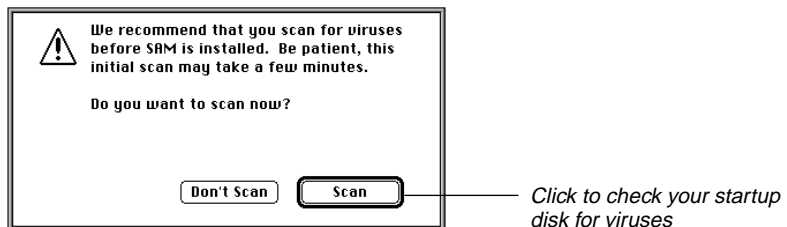
- 2 Double-click the install icon.
A screen identifying the product appears.
- 3 Click Continue.
The SAM Install dialog box appears (Figure 1-2).

Figure 1-2

- 4 Click Install.

NOTE: If an alert box appears telling you that installation cannot take place while other applications are running, either click Continue to close the other applications and continue installation, or click Cancel to exit the installer.

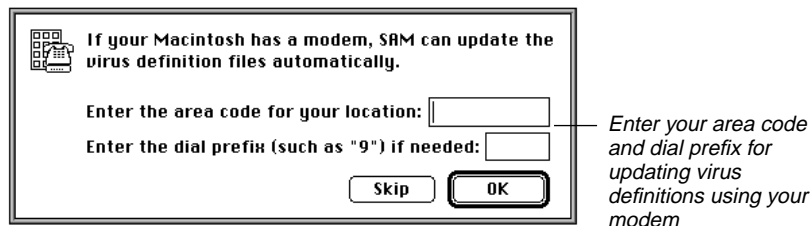
A scan dialog box appears (Figure 1-3).

Figure 1-3

- 5 Click Scan to scan the hard disk for viruses before SAM is installed.

A summary of the scan appears. If a virus was found, the SAM installer will allow you to repair the infected files. For detailed information about repairing infected files, see [“Repairing Infected Files,”](#) on page 42. After the scan is completed, the SAM files are copied to your hard disk. Then, the dialog box shown in Figure 1-4 appears.

Figure 1-4



- 6 Enter your area code in the **Area Code** text box. Then enter a dial prefix if necessary in the **Prefix** text box and click OK. This information is used to update virus definitions via modem.

If you don't have a modem, click Skip.

When the installation is complete, a dialog box appears to inform you that the installation was successful.

- 7 SAM displays a panel explaining SafeZones to make sure newly downloaded files are scanned for viruses automatically. See [“Specifying SafeZones,”](#) on page 94, for more information.
- 8 Click Restart to activate SAM.

Performing a Custom Install

You can also use the SAM installer to install selected components of SAM. For example, if your computer is short on memory (RAM), you can install a version of the automatic protection feature called SAM Intercept Jr., which requires less memory than the standard automatic protection feature called SAM Intercept.

To install selected components of SAM:

- 1 Insert the SAM Install #1 disk into your floppy drive.
A window displaying the disk contents opens automatically (see Figure 1-1).
- 2 Double-click the install icon.

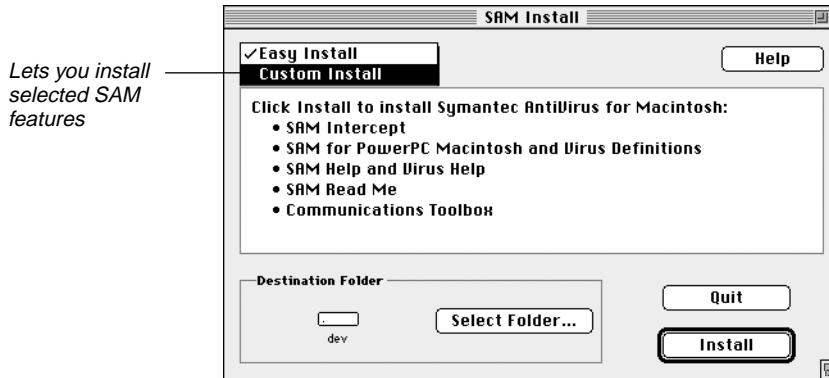
A screen identifying the product appears.

- 3 Click Continue.

The SAM Install dialog box appears (see Figure 1-2).

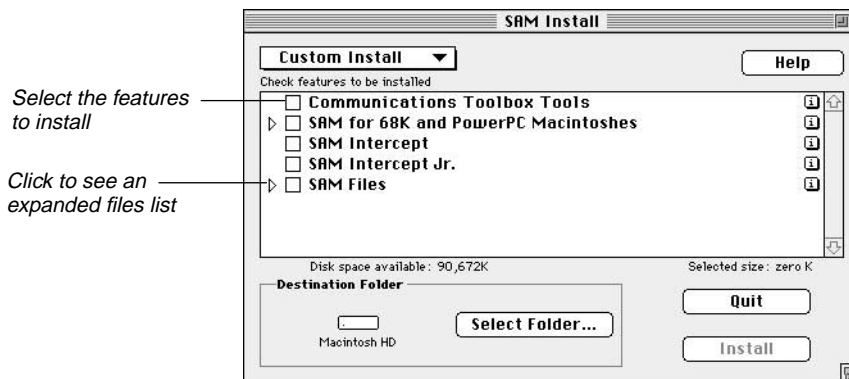
- 4 Select **Custom Install** from the pop-up menu (Figure 1-5).

Figure 1-5



The components you can select are shown in the SAM Install dialog box (Figure 1-6).

Figure 1-6



- 5 Check the appropriate check boxes for the components of SAM you want installed.

Communications Toolbox Tools: Installs files that are needed for updating virus definitions via modem.

SAM for 68K and PowerPC Macintoshes: Installs SAM files for use on PowerPC Macintosh computers in native mode and 68K Macintosh computers (all non-PowerPC Macintosh computers).

SAM Intercept: Installs the automatic protection feature of SAM that loads into memory at startup to guard your computer against viruses.

SAM Intercept Jr.: Installs a version of automatic protection that is similar to SAM Intercept, but does not monitor for suspicious activities. SAM Intercept Jr. takes less memory than SAM Intercept and cannot be customized.

If your computer has less than 2MB of RAM, select this option.

NOTE: Select either SAM Intercept or SAM Intercept Jr., but not both.

SAM Files: Installs supplementary files. Click the triangle to see a list of files to choose from.

NOTE: The SAM Virus Definitions file must be installed with any SAM components you choose.

6 Click Install.

TIP: Double-click the SAM 4.5 Read Me file you just installed and read it before going further. This file contains information about SAM that was not available at the time this manual was printed.

Where to Go After Installation

Now that you've installed SAM:

- You should scan all of your disks (including floppy disks) to make sure they are all virus-free. See [“Checking for Viruses,”](#) on page 31, for more information.
- You can learn more about preventing viruses from attacking your computer by reading [“Taking Precautions Against Viruses,”](#) on page 51.
- When you use the preset options, SAM is set up to protect your computer against viruses from the time your computer starts up and while you work in other applications. For information on customizing SAM protection, see [“Customizing SAM,”](#) on page 77.

Getting Started

2

Symantec AntiVirus for Macintosh is the most comprehensive virus prevention, detection, and elimination software available for your computer.

Here's what SAM does automatically:

- Checks applications for viruses at the time you run them
- Checks floppy disks for viruses when you insert them into a drive
- Monitors your Macintosh for any activity that might indicate the presence of a virus
- Check files for viruses when they are downloaded from the Internet

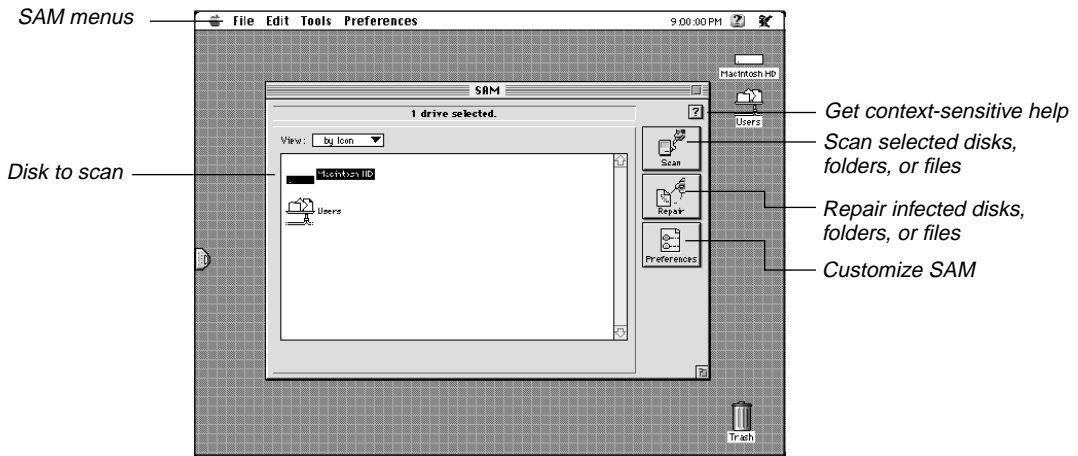
When you perform an easy installation of SAM, the automatic protection features listed above are already turned on.

Here's what you can do with SAM:

- Scan disks, folders, or files for viruses on demand
- Schedule virus scans to occur at specified times
- Protect applications from being infected by unknown viruses
- Update virus definitions
- Customize SAM to fit your virus-prevention needs

Figure 2-1 shows the SAM Main Window on the desktop.

Figure 2-1



Answers to Virus Questions

What are computer viruses?

A *computer virus* is a parasitic program written intentionally to alter the way your computer operates without your permission or knowledge. A virus attaches copies of itself to other files, and when activated, may damage files, cause erratic system behavior, or merely display messages.

Some viruses are programmed specifically to damage the data on your computer by corrupting programs, deleting files, or erasing your entire hard disk. Many of the currently known Macintosh viruses are not designed to do any damage. They simply replicate themselves and may display messages. However, because of bugs (programming errors) within the virus, an infected system may behave erratically or crash unexpectedly.

For more information on viruses and how they work, see “[About Computer Viruses](#),” on page 107. For information on a particular virus, see online help.

What are known and unknown viruses?

A *known virus* is one that can be detected and identified by name. An *unknown virus* is one for which SAM does not yet have a definition. SAM can protect your computer from both types of viruses.

How do viruses spread?

A virus is inactive until you execute an infected application or start your computer from a disk that has infected system files. Once a virus is active, it loads into your computer's memory and, at the very least, attaches copies of itself to other applications or system files on disks you access.

Viruses behave in different ways. Some viruses stay active in memory until you turn off your computer. Other viruses stay active only as long as the infected application is running. Turning off your computer or exiting the application removes the virus from memory, but it does *not* remove the virus from the infected file or disk.

Is my computer virus-free?

Use SAM to scan your disks for viruses. If a virus is found, SAM steps you through the process of eliminating the virus.

For more information, see [“Checking for Viruses,”](#) on page 31.

Is my computer protected against viruses?

If you installed SAM with all of the default options, your computer is automatically protected from viruses as soon as you start it. SAM Intercept loads into memory when your computer starts up, providing constant protection while you work.

SAM Intercept checks programs for viruses as they are run and monitors your computer for any activity that might indicate the presence of a virus. When a virus or “suspicious” activity (an event that could be the work of a virus) is detected, SAM Intercept tells you exactly what is happening. If a virus is found, SAM steps you through the process of eliminating it.

For more information, see [“Taking Precautions Against Viruses,”](#) on page 51, and [“Customizing SAM,”](#) on page 77.

Have I done everything I can?

Here's a list of important steps you can take to combat computer viruses:

- Scan your disks for viruses and eliminate any that are found. Also scan any other disk before you use it.

For instructions, see [“Checking for Viruses,”](#) on page 31.

- Make sure SAM Intercept is on at all times to prevent your computer from becoming infected. SAM Intercept is already turned on unless you specifically turn it off.

For more information, see “Turning SAM Intercept Off and On,” on page 27.

- Update virus definitions regularly so that you get maximum protection against new viruses.

For more information, see “Keeping Up with New Viruses,” on page 63.

Starting and Exiting SAM

Although SAM Intercept (the automatic protection feature) constantly protects your computer against viruses, there will be times when you need to take action. For example, you should run the SAM application when you want to:

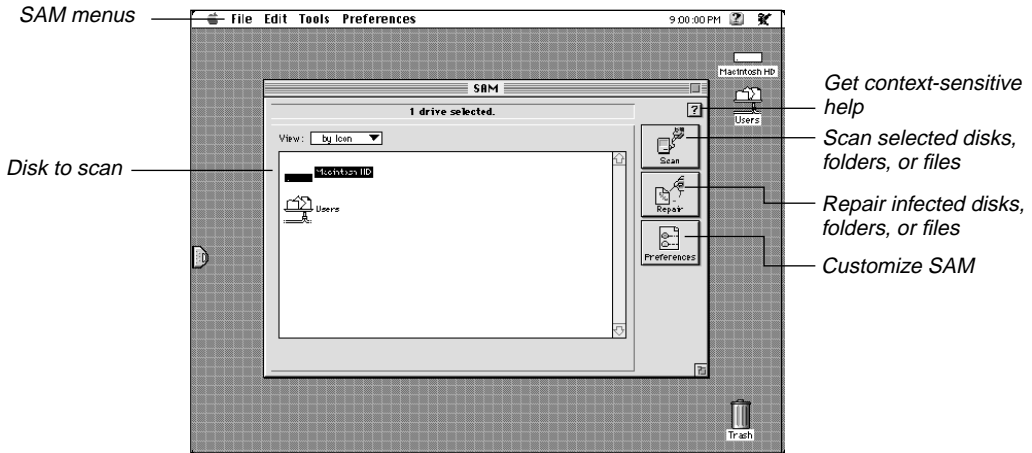
- Scan disks on demand
- Schedule unattended scans
- Eliminate viruses from infected files
- Update virus definitions
- Customize virus protection options

To start SAM:

- Double-click the SAM icon located in the SAM Folder.

The SAM Main Window appears (Figure 2-2).

Figure 2-2



TIP: For information on the tasks SAM can perform, skim the table of contents at the front of this manual.

To exit SAM:

- Choose QUIT from the File menu.

Turning SAM Intercept Off and On

SAM Intercept guards against viruses as soon as your computer starts up. It works like a sentry in the background, alerting you when it detects an infected file or suspects the presence of a virus. When you install SAM using the preset options, SAM Intercept is already turned on. It will load into your computer's memory each time you start up your Macintosh and provide constant protection while you work.

Although we don't recommend it, you may need to turn SAM Intercept off for a period of time (when troubleshooting extension conflicts, for example).



Turning SAM Intercept off drastically reduces protection against viruses. Make sure you turn it back on as soon as possible!

To turn SAM Intercept off:

- Choose TURN INTERCEPT OFF from the Preferences menu.
The menu command changes to TURN INTERCEPT ON.

To turn SAM Intercept back on:

- Choose TURN INTERCEPT ON from the Preferences menu.

Getting Help

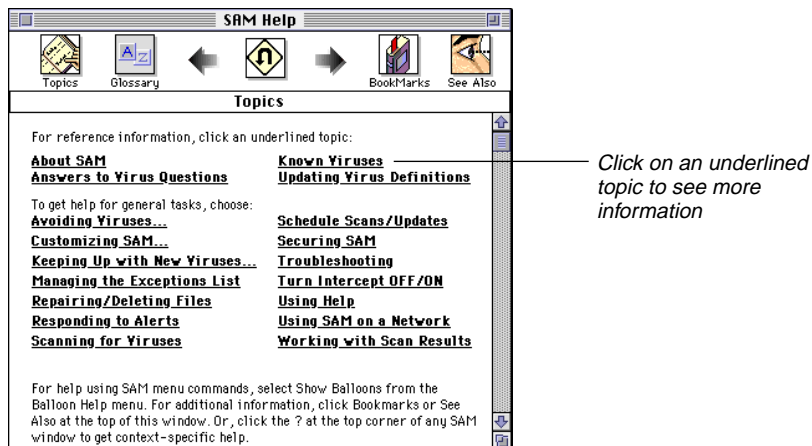
SAM comes with an extensive online help system that you can use to get immediate information about any of the features of SAM.

The help system includes an extensive topics list, a glossary, and several special features, including instant access to related information through underlined words or phrases. You can also establish bookmarks, which give you quick access to information you consult frequently. A “See Also” list of associated topics is available for many terms and concepts.

To use SAM help:

- Choose SAM HELP from the Help menu.
The SAM Help window appears (Figure 2-3).

Figure 2-3



You can also get context-sensitive help pertaining to a specific SAM dialog box or window that is open.

To get context-sensitive help:

- Click the help button in the upper right-hand corner of a dialog box or window (Figure 2-4).

Figure 2-4



Click the help button to get help about a particular window or dialog box

At the top of each help window, there are icons that function as follows:



Topics

Displays a list of help topics.



Glossary

Displays a list of glossary terms.



BookMarks

Displays a list of bookmarks. You can also create and delete bookmarks.

To create a bookmark for the topic currently shown in the help window, choose the appropriate number from the Set Bookmark pop-up menu.

To delete a bookmark, choose the appropriate bookmark number from the Clear Bookmark pop-up menu.



See Also

Displays a list of related topics.



Goes to the previous help page.



Goes to most recent help screen displayed.



Goes to the next help page.

Using Balloon Help

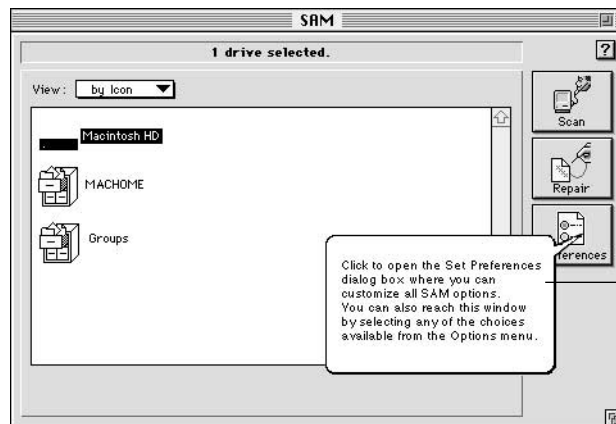
You can also use Balloon Help to familiarize yourself with the menu commands and dialog box options in SAM. With Balloon Help turned on, a descriptive text balloon appears when you move the cursor over a dialog box option, menu, or window item.

To turn Balloon Help on:

- Choose SHOW BALLOONS from the Help menu.

A text balloon pops up when you move the cursor over an item for which Balloon Help is available (Figure 2-5).

Figure 2-5



Balloon Help provides descriptive text about items in a window, dialog box, or menu

To turn Balloon Help off:

- Choose HIDE BALLOONS from the Help menu.

Checking for Viruses

3

Viruses activate when you launch an infected application, start your computer from a disk that has infected system files, or access a floppy disk with infected desktop files. With SAM you can scan any file, folder, or disk for viruses.

You can customize the way that SAM performs scans. For more information, see “[Customizing SAM](#),” on page 77.

NOTE: SAM can check compressed files for viruses, but not encrypted files. Encrypted files must be decrypted before you scan them. For information on which compressed file types SAM scans, see “[Selecting File Compression Options](#),” on page 93.

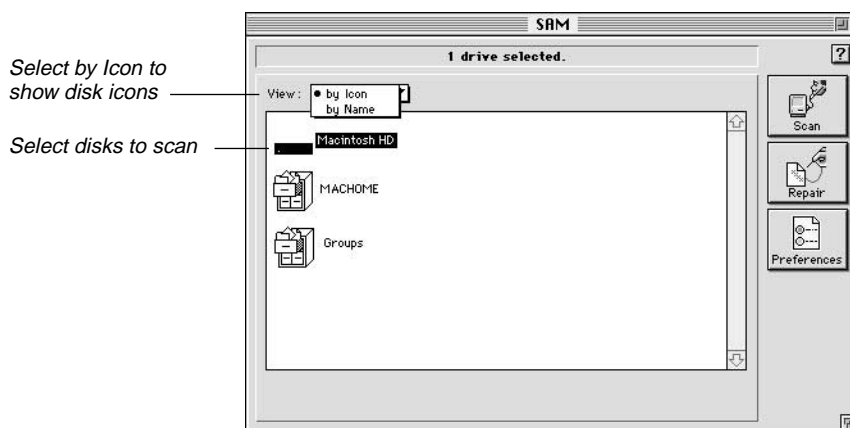
Scanning Disks

You should scan all disks before you use them to make sure they are virus-free.

To scan entire disks for viruses:

- 1 Select **by Icon** from the pop-up menu in the SAM Main Window (Figure 3-1).

Figure 3-1



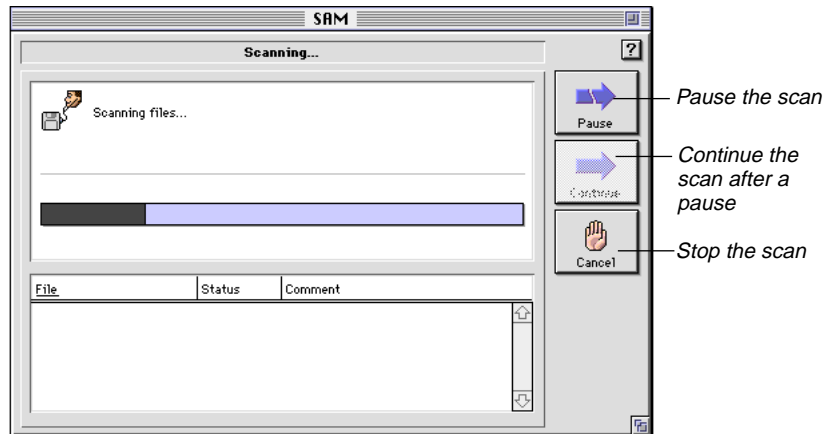
- 2 Select the disks you want to scan from the list of disk icons.

TIP: To select more than one disk icon, press Shift when you click the icons. To select all of the disk icons, choose SELECT ALL from the Edit menu.

- 3 Click Scan.

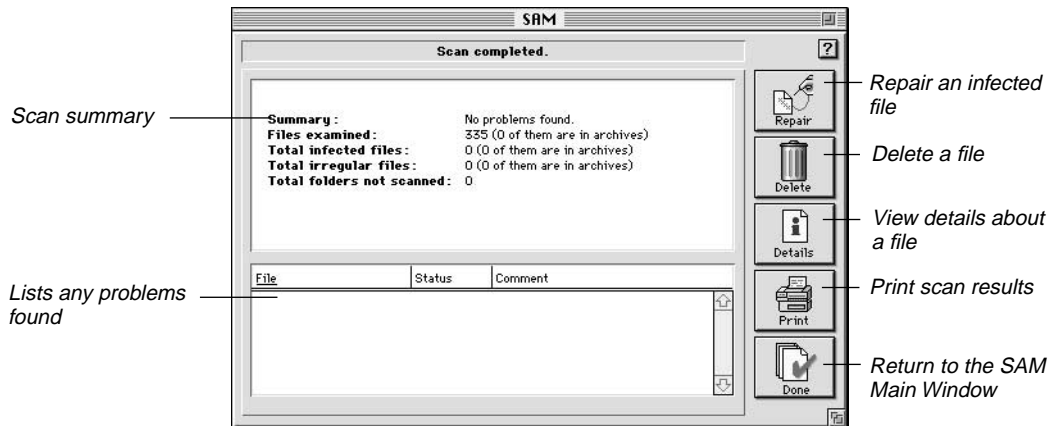
The scan window shows the progress of the scan (Figure 3-2).

Figure 3-2



When the scan is complete, the results of the scan are shown in the scan results window (Figure 3-3). The top portion of the screen shows a summary of the scan. The bottom portion of the screen lists any files that were found to have problems.

Figure 3-3



Problems Found

If a virus was found, don't panic—the virus can be removed. See [“Eliminating Viruses,”](#) on page 40, for instructions on how to proceed.

If any file irregularities are reported (such as messages about non-standard files), it does not necessarily mean the file is infected with a virus. See [“Resolving File Irregularities,”](#) on page 44, to determine whether the irregularity is a problem or not.

No Problems Found

If no problems were found during the scan, the scan results window shows summary information. See [“Working with Scan Results,”](#) on page 36, for more information.

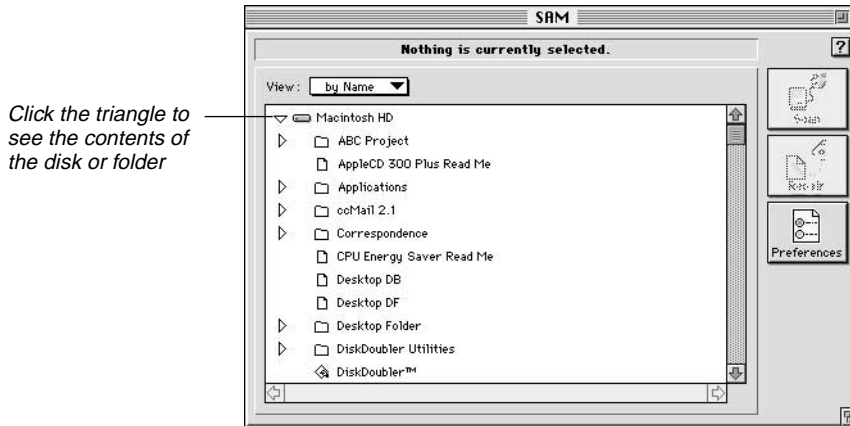
Scanning Folders and Files

Before copying files to your hard disk, scan them for viruses. You can scan any combination of files, folders, or disks.

To scan folders and files:

- 1 Select **by Name** from the pop-up menu (see Figure 3-1).
The disk names appear (Figure 3-4).

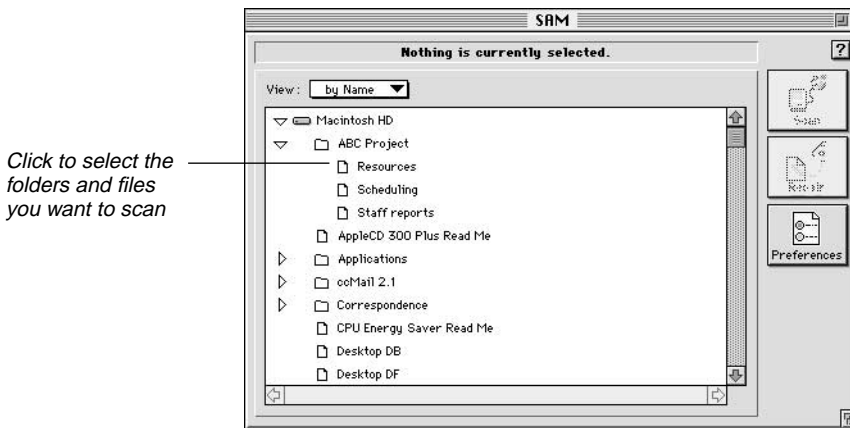
Figure 3-4



- 2 Click the triangle next to the disk name to view the contents of the disk.

A list of folders and files appears (Figure 3-5).

Figure 3-5



- 3 Select the folders or files you want to scan. To scan an entire disk, select the disk name.

TIP: To select more than one file or folder, press Shift when you click the item. To select all disks, choose SELECT ALL from the Edit menu.

4 Click Scan.

The results of the scan are shown in the scan results window (see Figure 3-3).

Problems Found

If a virus was found, don't panic—the virus can be removed. See “[Eliminating Viruses](#),” on page 40, for instructions on how to proceed.

If any file irregularities are reported (such as messages about non-standard files), it does not necessarily mean the file is infected with a virus. See “[Resolving File Irregularities](#),” on page 44, to determine whether the irregularity is a problem or not.

No Problems Found

If no problems were found during the scan, the scan results window shows summary information. See “[Working with Scan Results](#),” on page 36, for more information.

Scanning Multiple Floppy Disks

If you have many floppy disks or other removable media to scan in one sitting, you can use the SCAN & EJECT command to make the process go faster. At the end of each scan, the removable media item is ejected automatically so you can insert the next one.

To scan multiple floppy disks or other removable media:

- 1 Choose SCAN & EJECT from the Tools menu.
A message appears in the SAM Main Window instructing you to insert the disk you want to scan.
- 2 Insert a floppy disk or other removable media.
The results of the scan are shown in the scan results window (see Figure 3-3).
- 3 Repeat step 2 for all the removable media items that you want to scan.
- 4 Click Done to end the scan.

Problems Found

If a virus was found, don't panic—the virus can be removed. See “[Repairing Multiple Floppy Disks](#),” on page 43, for information on how to proceed.

If any file irregularities are reported (such as messages about non-standard files), it does not necessarily mean the file is infected with a virus. See “[Resolving File Irregularities](#),” on page 44, to determine whether the irregularity is a real problem or not.

No Problems Found

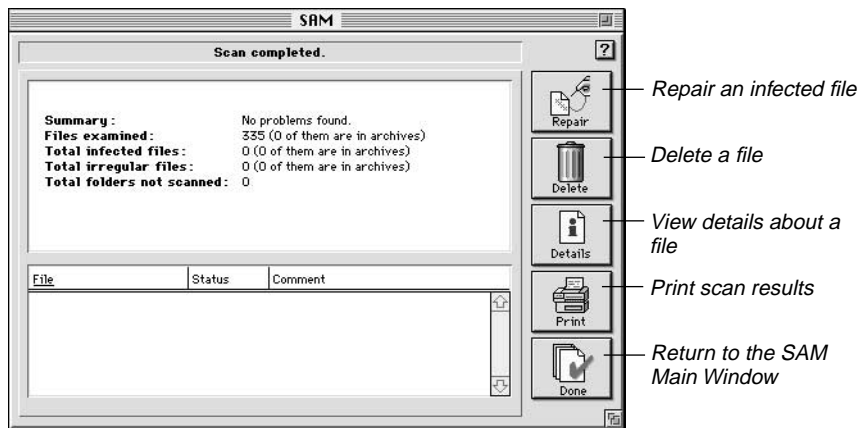
If no problems were found during the scan, the scan results window shows summary information. See “Working with Scan Results” next for more information.

Working with Scan Results

When the scan is complete, the scan results window displays summary information about the scan that was performed (Figure 3-6).

NOTE: If a virus was found, see “[Eliminating Viruses](#),” on page 40, for information on how to proceed.

Figure 3-6



Printing a Scan Report

You can print the scan results for future reference.

To print the scan report:

- Click Print in the scan results window.

Or,

Choose PRINT REPORT... from the File menu.

A standard Print dialog box appears, allowing you to change the printing options before printing the scan results.

Saving a Scan Report to a File

You can save a report of the scan results to a file and view it later.

To save the scan report to a file:

- Choose SAVE REPORT AS... from the File menu.

A standard file dialog box appears where you can specify a name and location for the file. The default filename is "SAM Report *date*," where *date* is the date of the scan.

NOTE: For information on the report's file format and other report options, see "[Customizing Reporting Options](#)," on page 88.

Taking Corrective Action

4

This chapter helps you resolve problems detected by SAM, such as a virus or suspicious activity on your computer.

What to Do Next

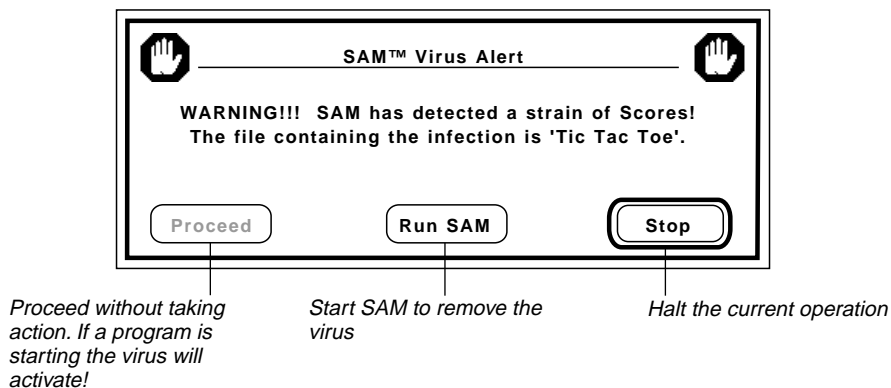
Skim this chapter to find the section title or picture that best describes the problem reported on your screen; then follow the instructions provided.

If the message on your screen is not discussed in this chapter, see “[System Messages](#),” on page 121, for more information.

Responding to Virus Alerts

When a SAM Virus Alert appears on your screen, the name of the file and the name of the virus are shown in an alert box (Figure 4-1).

Figure 4-1



To respond to the virus alert:

- Click Run SAM to open the SAM Main Window so that you can remove the virus.

The file is scanned again and the results are shown in the scan results window. See “[Eliminating Viruses](#),” on page 40, for instructions on how to remove the virus.

Or,

- Click Proceed to continue without taking action.

If the Proceed button is dimmed, SAM is configured not to allow infected applications to run. This is the default setting.



Use caution when selecting the Proceed button. The virus will activate and spread to other files.

Or,

- Click Stop to halt the current operation.

Or,

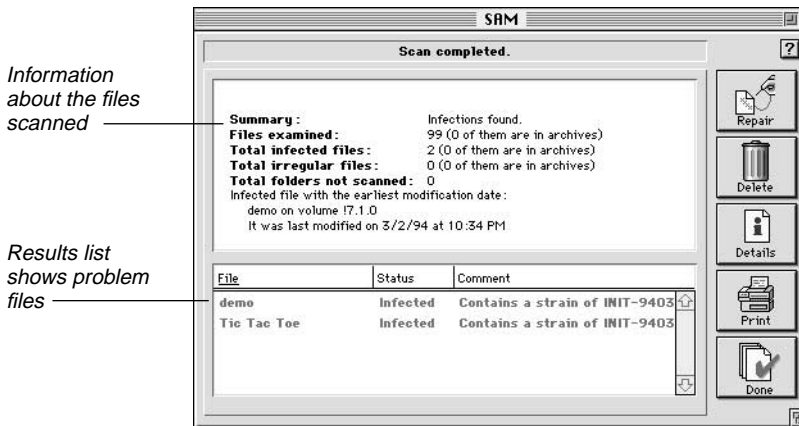
Click Eject if the virus was found on a floppy disk.

Eliminating Viruses

NOTE: If you have come to this section because a virus alert appeared on your screen, click Run SAM in the SAM Virus Alert box. SAM will scan the file and display the scan results window (see Figure 4-2).

When SAM finds a virus, the name of the infected file and the name of the virus are shown in the results list window (Figure 4-2).

Figure 4-2



Don't worry, the virus can be removed by either deleting or repairing the infected file.

Deleting versus Repairing

If you have an uninfected backup copy of a file, we recommend deleting the infected file and replacing it with an uninfected copy. Sometimes viruses damage a file beyond repair.

If you do not have an uninfected backup copy of the file, you can attempt to repair it. Always delete any *Trojan horse* programs that SAM reports.

TIP: Double-click the infected file in the scan results window to see a dialog box that lets you either delete or repair the file.

Deleting Infected Files

You can eliminate the virus by deleting the infected file. Then you can replace the file with an uninfected copy.

To delete an infected file:

- 1 Select the file or files you want to delete in the results list (see Figure 4-2).
- 2 Click Delete.

A dialog box appears asking you to verify the deletion (Figure 4-3).

Figure 4-3



- 3 Click OK.

The Status column in the results list shows “Deleted” for the file.

After Deleting Files

After deleting infected files, scan your hard disks and floppy disks with SAM to verify that there aren't any other files that contain viruses. Once you are certain that your system is virus-free, replace the files you deleted with uninfected copies. Make sure you scan the replacement files before copying them to your hard disk.

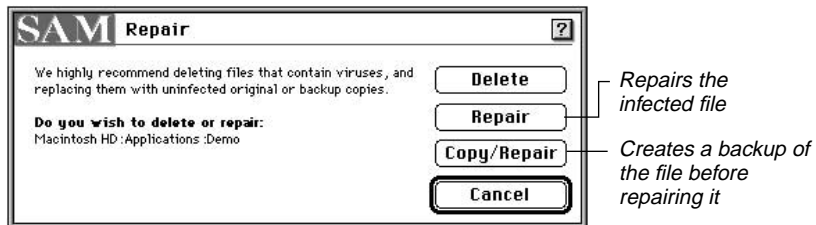
Repairing Infected Files

Repairing an infected file removes the virus and returns the file to its original state.

To repair an infected file:

- 1 Select the file or files you want to repair in the results list (see Figure 4-2).
- 2 Click Repair.
Or,
Double-click the selected file or files.
A repair dialog box appears (Figure 4-4).

Figure 4-4



- 3 Click Repair.
Or,
Click Copy/Repair if you want a backup copy of the file created before it is repaired.
The Status column in the results list shows "Repaired" for the file.

After Repairing Files

After repairing infected files, scan your hard disks and floppy disks again with SAM to verify that there aren't any other infected files. Then check the repaired files to make sure they function properly. For example, if you repaired a word processing program, start it, edit a file, save a file, and so forth to make sure it has been repaired correctly.

NOTE: If you chose to have SAM make a backup copy of the infected file before you repaired it, be sure to delete the backup file (because it too is infected) once you are certain the repair worked correctly. The infected backup copy of the file is stored in the same directory as the original file. (The backup copy is named "Copy of *filename*" where *filename* is the name of the original file.)

Repairing Multiple Floppy Disks

If you have several infected floppy disks or other removable media to repair, you can use the REPAIR & EJECT command to make the process go faster. After a floppy disk or other removable media item is repaired, the item is ejected so you can insert the next one.

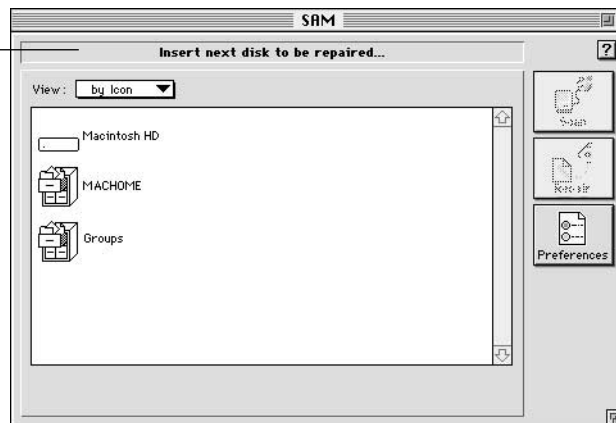
To repair multiple floppy disks:

- 1 Choose REPAIR & EJECT from the Tools menu.

A message appears instructing you to insert the item you want to repair (Figure 4-5).

Figure 4-5

SAM instructs you to insert the infected disk



- 2 Insert the floppy disk or other removable media item.

The scan window shows the progress of the scan. When the scan is complete, the results of the repair are shown in the scan results window (see Figure 4-2).

- 3 Repeat step 2 for the other items to repair.

NOTE: See “[After Repairing Files](#),” on page 43, for information on what to do once the repair is complete.

What to Do if Repair Is Unsuccessful

Sometimes viruses damage a file beyond repair. If SAM could not repair the infected file, you must delete the file to remove the virus. After you delete the infected file, you can replace it with an uninfected copy. See “[Deleting Infected Files](#),” on page 41, for information, tips, and cautions regarding this operation.

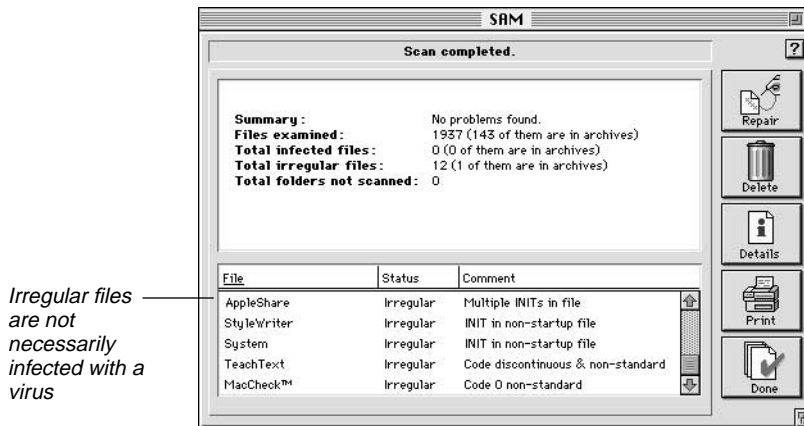
Resolving File Irregularities

Irregular files have characteristics that are “odd” or “abnormal.” Although irregularities reported in a file may indicate the presence of a virus, they do *not* necessarily mean the file is infected. Some programs legitimately have irregular characteristics.

NOTE: For information on the specific file irregularity reported, see “[System Messages](#),” on page 121.

When SAM detects an irregular file during a scan, the name of the file appears in the scan results list (Figure 4-6).

Figure 4-6



It is not always easy to figure out whether a file irregularity is a problem. In many cases, reports of file irregularities are false alarms. However, on the chance that the file has a problem, you should check it out. The procedure below provides some guidelines for investigating file irregularities.

TIP: If the application program flagged as irregular has been scanned in the past without file irregularities reported, and you haven't changed the program (by upgrading to a new version, for example), then the program may have a problem.

To investigate file irregularities:

- 1 Choose SCAN... from the Preferences menu, then check **Skip known irregularities** in the Set Preferences dialog box.

This instructs SAM not to report on file irregularities that are known to be legitimate.

- 2 Scan the irregular file again to see if the irregularity has been resolved.

If the file irregularity is reported again, go to step 3.

- 3 If you're confident that the original application disk (the disk that came in the shrink-wrapped box) has not been used by other computers, and has remained locked, scan the *locked* disk to see if it too has an irregularity. If SAM reports an irregularity on the original disk, then it's likely that the file does not have a problem.

If the original disk does not show the file irregularity, delete the file from your hard disk and replace it with a new copy from the original disk.

If you're not confident that the application is intact, then go to step 4.

- 4 Get the latest virus definitions file, then scan the file again. If the application does contain a virus, the newest virus definitions file may have a definition for it.

See “[Keeping Up with New Viruses](#),” on page 63, for more information on updating the virus definitions file.

Viewing File Details

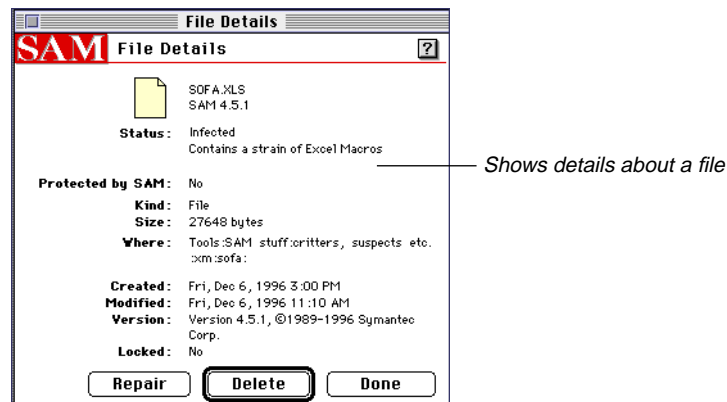
If SAM reports a problem with a file (such as a virus), you can view details, including the file type, size, location, date created, and date modified.

To view file details:

- 1 Select the file in the scan results window (see Figure 4-2).
- 2 Click Details.

The File Details dialog box appears (Figure 4-7).

Figure 4-7



- 3 If the file is infected with a virus, you can click Delete to delete the file.

Or,

Click Repair to repair the infected file.

NOTE: If the repair is not successful, you must delete the file to remove the virus.

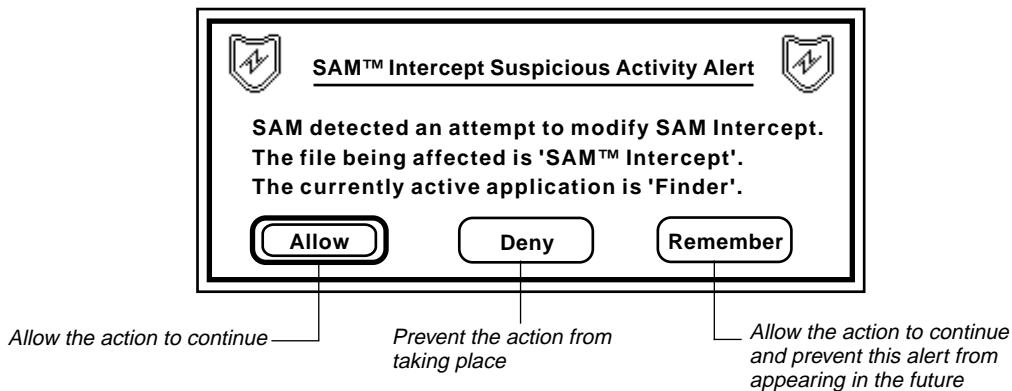
- 4 Click Done.

NOTE: If you deleted an infected file, see “[After Deleting Files](#),” on page 42, for more information. If you repaired an infected file, see “[After Repairing Files](#),” on page 43, for more information.

Responding to Suspicious Activity Alerts

A *suspicious activity* is an activity that viruses often perform when spreading or damaging your files. A suspicious activity alert does *not* necessarily mean a virus is present. The suspicious activities reported are often legitimate. However, because they are actions that viruses also perform, you should investigate them. When a suspicious activity is detected, an alert box similar to the one in Figure 4-8 appears.

Figure 4-8



For a description of each suspicious activity that SAM can detect, see “[Customizing Suspicious Activity Monitoring](#),” on page 80.

To respond to a suspicious activity alert:

- If the message in the alert box describes an activity that is valid in the context of the application you are running, click Allow to continue the operation.

For example, if you are copying a file using Finder and receive an alert stating that there is an attempt to create an application, click Allow.

Or,

- If the alert box appears unexpectedly or does not seem to apply to what you are attempting to do, click Deny to prevent the action from taking place.

For example, if you are playing a game and receive an alert stating that there is an attempt to format your hard disk, click Deny.

If the Deny button is dimmed, the suspicious activity has proceeded too far for SAM to stop without causing damage or “crashing” the system. If this happens, note the file involved and the currently active application before continuing. Then scan both files to check for known viruses.

Or,

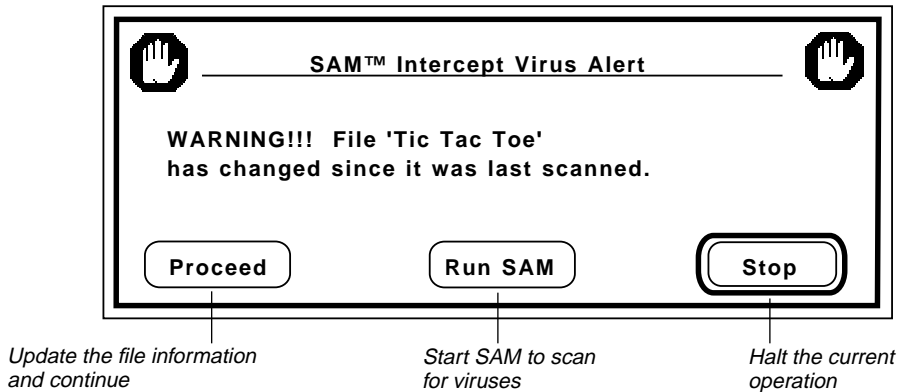
- If the activity is valid in the context of the application you are running and you don't want SAM to alert you of this activity (performed by this application) in the future, click Remember.

Clicking Remember adds this activity to the Exceptions List. Future attempts to perform the same action by the same application will not trigger the suspicious activity alert. See “[Managing the Exceptions List](#),” on page 57, for more information on viewing and editing the exceptions list.

Responding to File Changed Alerts

A SAM Intercept alert similar to the one shown in Figure 4-9 appears when an application file has changed since the last time it was scanned. Changes to application files could indicate the presence of an unknown virus. However, they do *not* necessarily mean the file is infected. Although it's unusual, sometimes applications modify themselves.

Figure 4-9



TIP: If you have been using the application for some time without an alert of this kind appearing, the file is more likely to have a problem.

To resolve a file changed alert:

- If you are certain the application file has changed for legitimate reasons (for example, you recently installed a new version of the application), click Proceed.

If the Proceed button is dimmed, SAM is configured not to allow the application to run. This is the default setting.

Or,

- If you are uncertain about the file, click Stop to prevent the application from running. Then delete the file and replace it from the *locked* original application disk (the disk that came in the shrink-wrapped box).

Or,

- Click Run SAM to automatically rescan the file.

TIP: Make sure you have the most recent virus definitions file. If the application does contain an unknown virus, the newest virus definitions file may have a definition for it. See [“Keeping Up with New Viruses,”](#) on page 63, for more information on updating the virus definitions file.

Taking Precautions Against Viruses

5

This chapter discusses some important precautions you can take to protect your computer from viruses. This chapter explains how to:

- Schedule automatic virus scans
- Schedule automatic virus definition updates
- Protect against unknown viruses
- Create a decontamination disk

Avoiding Viruses

Viruses spread when you start up your computer from an infected disk (hard or floppy) or when you run an infected application program.

To avoid viruses, follow these guidelines:

- Always scan disks before you use them. See “[Checking for Viruses](#),” on page 31.
- Keep SAM Intercept turned on at all times to prevent viruses from infecting your computer.

SAM Intercept is already turned on when you install SAM using the preset options.

- Safeguard your computer from unknown viruses by using the protection features to monitor for suspicious activities. See “[Protecting Against Unknown Viruses](#),” on page 56.
- Update virus definitions regularly. See “[Scheduling Virus Definition Updates](#),” on page 54, or “[Keeping Up with New Viruses](#),” on page 63.
- Back up your files regularly and keep more than just the most recent backup. Also, make a backup copy of your uninfected System folder.
- Write-protect disks whenever practical.
- Schedule scans to occur automatically. See “[Scheduling Virus Scans](#),” on page 52.

Scheduling Events

To make virus prevention as easy as possible, SAM lets you schedule:

- virus scans to occur at specified times
- automatic updates of virus definitions via modem

NOTE: If your Macintosh is off during the time an event should take place, the event occurs the next time you start your Macintosh.

Scheduling Virus Scans

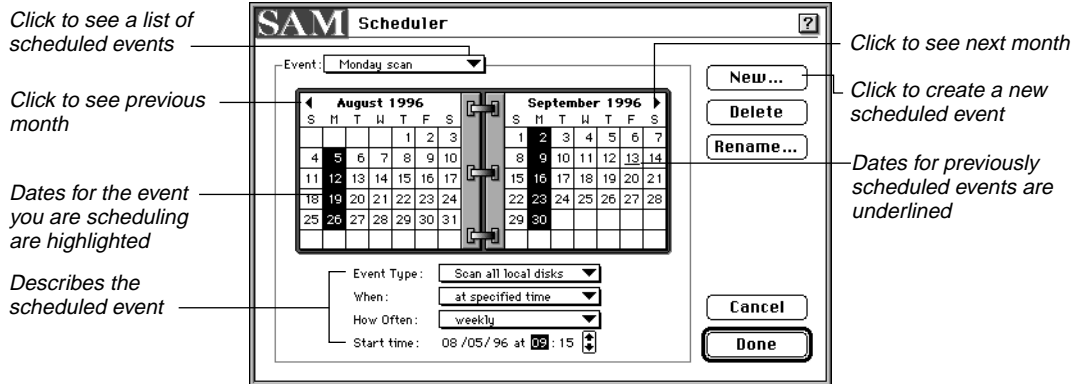
Follow the procedure below to schedule automatic virus scans.

To schedule virus scans:

- 1 Choose SCHEDULER... from the Tools menu.

The Scheduler dialog box appears (Figure 5-1).

Figure 5-1



- 2 Click New....

A dialog box appears prompting you to enter a name for the scheduled event.

- 3 Type the event name in the text box, then click OK.

- 4 Choose the item you want to scan from the **Event Type** pop-up menu.

Scan System folder: Scans the System folder on the startup disk.

Scan System disk: Scans the entire startup disk.

Scan all local disks: Scans all disks physically connected to your computer.

Scan all network disks: Scans all network drives mounted at the time the scan runs.

Scan all mounted disks: Scans all local and network drives mounted at the time the scan runs.

- 5 Choose when the scan should occur from the **When** pop-up menu.

At specified time: Lets you decide when the scan will occur.

At startup: Scans for viruses each time your computer starts up.

At shutdown: Scans for viruses each time your computer shuts down.

- 6 Choose the frequency of the scan from the **How Often** pop-up menu.

The days on which the scans will occur appear highlighted in the calendar. Dates for other scheduled events are underlined.

- 7 Finish scheduling the scan by entering the correct time and date information.

Click the hour text box and use the arrow keys to set the start hour. Then click the minute text box to set the start minute.

Start time: 08/05/96 at 09:15 

This option is dimmed if the scan will occur at startup or shutdown.

- 8 Click Done.

NOTE: The scan results are stored in a file called “SAM Report *date*” where *date* represents the date the scan occurred. You can view the file by double-clicking it.

For information on selecting an application for viewing these reports, see “Customizing Scan Reports,” on page 88.


Scheduling Virus Definition Updates

If you have a modem, you can schedule automatic updates to the virus definitions files. SAM first verifies that you don't already have the most recent virus definitions before updating the file.

TIP: Before scheduling automatic virus definitions updates, first make sure the update process works correctly by stepping through the process once. See [“Updating Virus Definitions Automatically,”](#) on page 66, for more information.

To schedule virus definition updates:

- 1 Choose SCHEDULER... from the Tools menu.
The Scheduler dialog box appears (see Figure 5-1).
- 2 Click New....
A dialog box appears prompting you to enter a name for the scheduled event.
- 3 Type the event name in the text box, then click OK.
- 4 Choose **Update Virus Definitions** from the **Event Type** pop-up menu.
- 5 Choose the frequency of updates in the **How Often** pop-up menu.
We recommend choosing **monthly**.
The days on which the updates will occur appear highlighted in the calendar. Dates for other scheduled events are underlined.
- 6 Finish scheduling the update by entering the correct time and date information.
Click the hour text box and use the arrow keys to set the start hour.
Then click the minute text box to set the start minute.

Start time: 08 /05 /96 at 09 : 15 
- 7 Click Done.

Editing Scheduled Events

You can easily make changes to the events you schedule.

To edit a scheduled event:

- 1 Choose SCHEDULER... from the Tools menu.
The Scheduler appears (see Figure 5-1).
- 2 Choose the scheduled event you want to change from the **Event** pop-up menu.
- 3 Make your changes.
For information on the options, see “Scheduling Virus Scans,” on page 52, or “Scheduling Virus Definition Updates,” on page 54.
- 4 Click Done.

Deleting Scheduled Events

You should delete events you no longer want.

To delete a scheduled event:

- 1 Choose SCHEDULER... from the Tools menu.
The Scheduler dialog box appears (see Figure 5-1).
- 2 Choose the scheduled event you want to delete from the **Event** pop-up menu.
- 3 Click Delete.

Protecting Against Unknown Viruses

An *unknown virus* is one for which SAM does not yet have a definition. You can protect files against unknown viruses by:

- Turning the **Protect against unknown viruses** feature on in Scan Options (it's on by default).

When SAM protects an application file, it records critical information about it (similar to taking a “fingerprint”). On subsequent scans, SAM checks the file against the “fingerprint” and notifies you if there are any changes that could indicate the presence of an unknown virus.

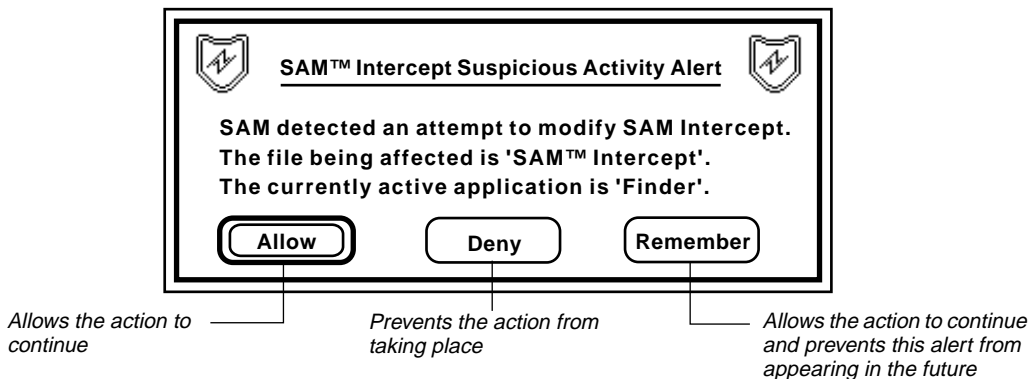
For information on enabling this feature, see “[Customizing Scanning Options](#),” on page 83.

- Monitoring for suspicious activities (activities that viruses sometimes perform).

Monitoring for Suspicious Activities

A *suspicious activity* is an activity that viruses sometimes perform when damaging your files or spreading through your system. Although some applications perform these actions for valid reasons, SAM can monitor for the activities on the chance that an unknown virus is performing one of them. Figure 5-2 shows an example of a suspicious activity alert.

Figure 5-2



If a suspicious activity is detected, it does *not* necessarily mean that a virus is performing the activity—you will decide whether the activity can continue or not. For example, if you are running a disk copying program and receive an alert stating that there is an attempt to format a drive, you want the action to continue because it is valid in the context of the application you are running. On the other hand, if you are playing a game and receive the same alert, you should not allow the activity to continue because it is not valid in the context of playing a game.

If you installed SAM using the preset options, the most common virus-like behaviors are monitored. To customize suspicious activity monitoring, see “Customizing Suspicious Activity Monitoring,” on page 80.



If a suspicious activity alert is displayed on your screen right now, see “Responding to Suspicious Activity Alerts,” on page 47, for instructions on how to proceed.

Managing the Exceptions List

The *Exceptions List* contains conditions or activities that would normally be flagged as suspicious, which you have told SAM to ignore.

For example, if you are using the Finder to copy an application and receive an alert warning that there is an attempt to create an application, you can tell SAM to not warn you of this particular action in the future. An Exception is saved when you click the Remember button in a suspicious activity alert. See “Customizing Alerts,” on page 85, for information on turning this feature on or off.

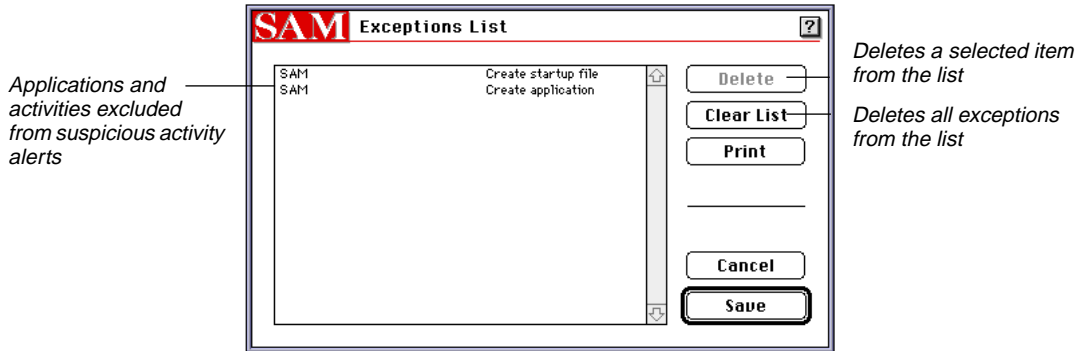
NOTE: If you rename an application, you must reestablish exceptions for the application by clicking the Remember button when SAM displays a suspicious activity alert.

Removing Entries from the List

You can remove exceptions you no longer need or want. For example, if you remove an application from your hard disk, you should remove the exceptions saved for that application.

To remove entries from the list:

- 1 Choose EDIT EXCEPTIONS LIST... from the Tools menu.
The Exceptions List dialog box appears (Figure 5-3).

Figure 5-3

- 2 Select the exception you want to delete.
If you want to select more than one exception, Shift-Click the exceptions.
- 3 Click Delete.
- 4 Click Save to save your changes.

Clearing All Entries from the List

You can remove all entries from the Exceptions List, if you ever need to. Be aware, however, that SAM will resume alerting you of suspicious activities when they occur.

To clear all entries from the list:

- 1 Choose EDIT EXCEPTIONS LIST... from the Tools menu.
The Exceptions List dialog box appears (see Figure 5-3).
- 2 Click Clear List.
- 3 Click Save.

Printing the Exceptions List

You can print the Exceptions List to use for future reference.

To print the Exceptions List:

- 1 Choose EDIT EXCEPTIONS LIST... from the Tools menu.
The Exceptions List dialog box appears (see Figure 5-3).
- 2 Click Print, then click Print again in the standard Print dialog box that appears.
- 3 Click Save to save any changes you made before printing.
Or,
Click Cancel to cancel any changes you made before printing.

Creating a Decontamination Disk

A Decontamination Disk is an important part of taking precautions against viruses—it contains SAM and the files your Macintosh needs to start up. If your Macintosh ever fails to start up or you think your computer is infected with a virus, you can use the Decontamination Disk to start up your computer again and remove any viruses if necessary.

NOTE: You don't need to create a Decontamination Disk if your Macintosh starts up from the Apple Macintosh CD.

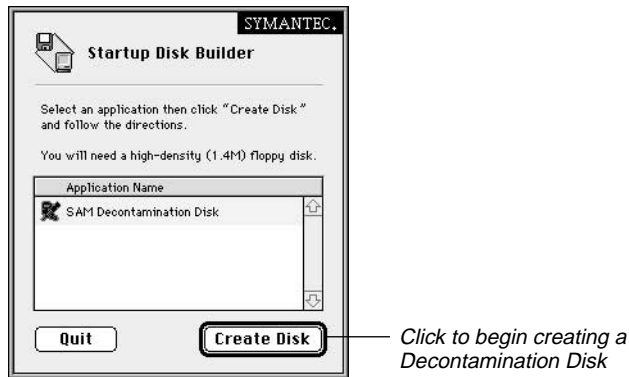
You will need:

- 1.4MB floppy disk
- SAM Install #2 disk
- Some computers require the Disk Tools disk (included with the System 7 installation disk set)

To create a Decontamination Disk:

- 1 Double-click the Startup Disk Builder icon in the SAM Folder.
The Startup Disk Builder dialog box appears (Figure 5-4).

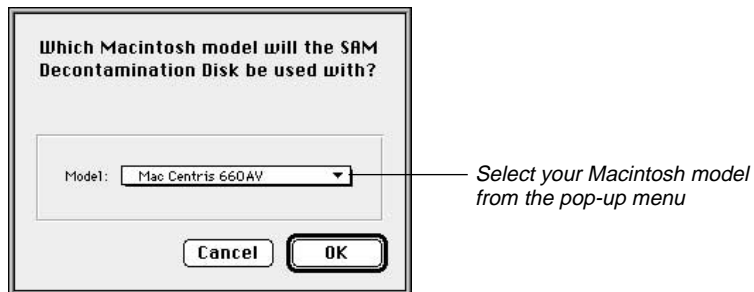
Figure 5-4



- 2 Click Create Disk.

A dialog box appears prompting for the Macintosh model (Figure 5-5).

Figure 5-5

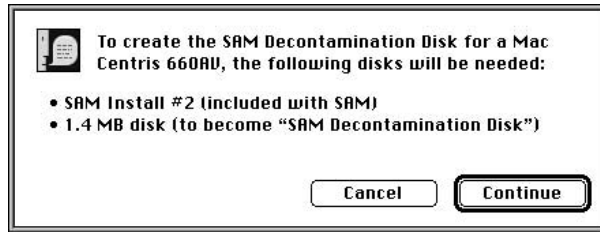


- 3 Choose the type of Macintosh you have from the **Model** pop-up menu, then click OK.

Choose **Other** if your Macintosh is not in the list, then follow the prompts on the screen to finish creating the Decontamination Disk.

A confirmation dialog box appears (Figure 5-6).

Figure 5-6



- 4 Click OK.
- 5 Follow the prompts on your screen to finish creating the Decontamination Disk.

NOTE: You will be prompted to swap disks several times during this process.

- 6 After the Decontamination Disk is created, write-protect it and store it in a safe place.

To write-protect the disk, slide the tab on the back of the disk to uncover the hole through the disk.

NOTE: When you update SAM virus definitions, be sure to copy the virus definitions file to your Decontamination Disk too. Remember to write-protect the Decontamination Disk after updating it.

Keeping Up with New Viruses

6

To keep newly discovered viruses from invading your computer, you will occasionally need to update the *SAM Virus Definitions* file. This file contains virus detection and repair information that allows SAM to recognize and alert you to specific viruses.

This chapter explains the various ways you can update virus definitions and view the list of viruses that SAM detects.

About the Virus Definitions Files

SAM uses two virus definitions files:

- SAM Virus Definitions file

This file comes with the SAM software package and provides SAM with information to find and repair viruses. These are also called *built-in definitions*.

- SAM User Definitions file

This file contains virus definitions that you enter manually from information provided by Symantec. SAM uses these virus definitions to detect newly discovered viruses, but not repair them. If a virus is detected in this manner, you must delete the file to remove the virus.

NOTE: If you update the SAM Virus Definitions file on a regular basis, you do not have to enter virus definitions manually.

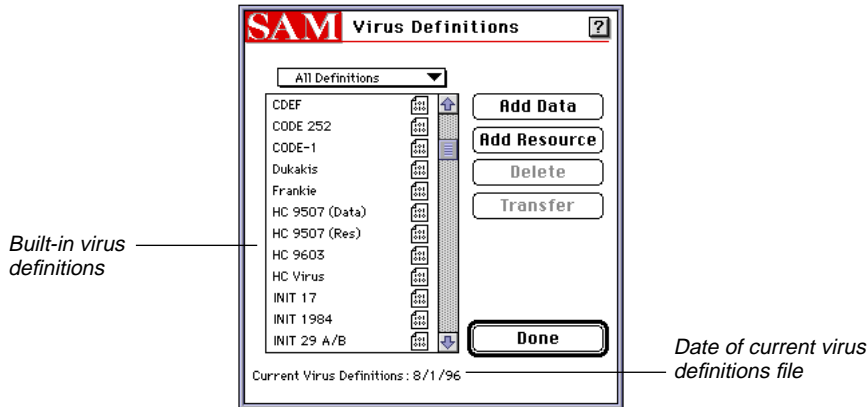
Viewing the Virus List

You can see which viruses SAM detects by using the EDIT VIRUS DEFINITIONS... command to view the list of virus names. You can view descriptions of known viruses, including their symptoms and aliases, using the online help system.

To view a list of virus names:

- 1 Choose EDIT VIRUS DEFINITIONS... from the Tools menu.
The Virus Definitions dialog box appears (Figure 6-1).

Figure 6-1



- 2 Select the category of viruses to display in the pop-up menu.

All Definitions: Displays all of the viruses that SAM can detect.

Built-in Definitions: Displays viruses that were installed with SAM or updated from update disks or from downloading the virus definitions.

User Definitions: Displays viruses that were entered manually. SAM can detect these viruses, but not repair them.

- 3 Click Done.

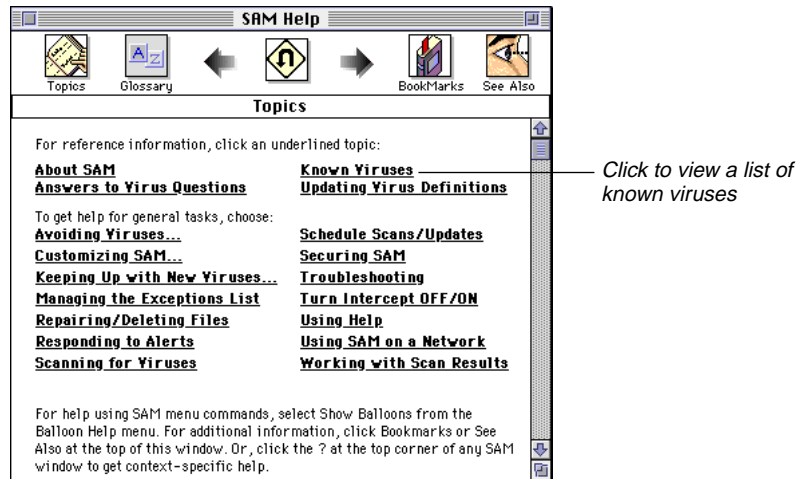
Viewing Virus Descriptions

You can use the online help system to view details about the viruses SAM detects, including the type of files they infect, their symptoms, and their aliases.

To view virus details in online help:

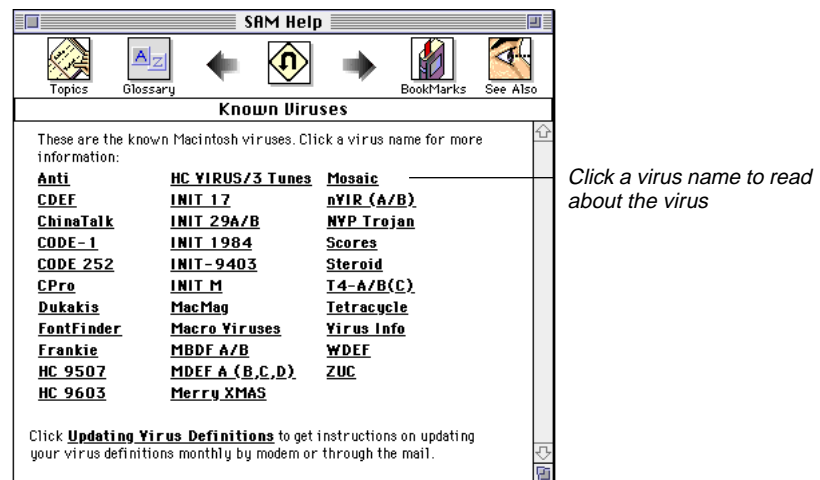
- 1 Choose SAM HELP from the Help menu.
The SAM Help window appears (Figure 6-2).

Figure 6-2



- 2 Click **Known Viruses** from the topics list.
A list of known viruses appears (Figure 6-3).

Figure 6-3



- 3 Click the appropriate virus name to view a detailed description.

Adding New Virus Definitions

To ensure that your computer is protected from new viruses, you should update the virus definitions files when new definitions become available. You can update virus definitions using any one of the following methods:

- Update virus definitions automatically (if you have a modem, this is the easiest method)
- Download virus definitions from a BBS (bulletin board system)
- Install a new virus definitions file from a Virus Definitions Update Disk
- Add virus definitions manually from information provided by Symantec (this method updates only the SAM User Definitions file)

TIP: You do not have to enter virus definitions manually if you download virus definitions by modem or install them from a virus update disk, because the new virus definitions, along with all previous virus definitions, will already be available to SAM.

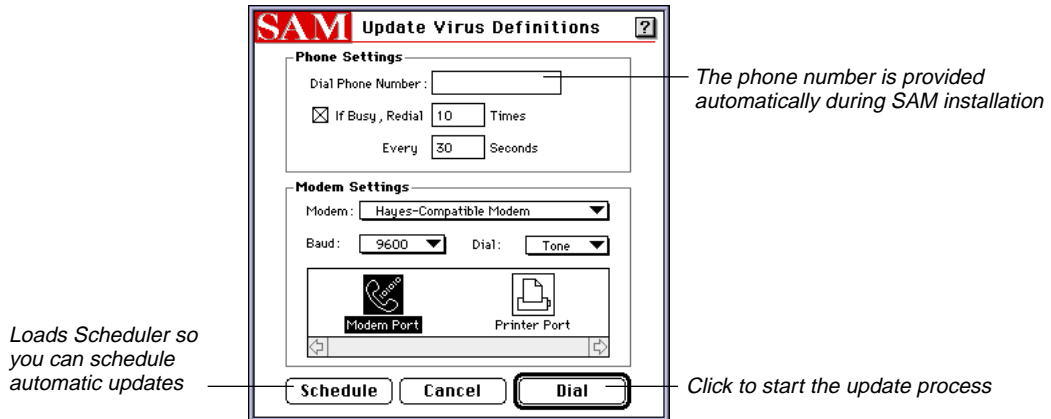
Updating Virus Definitions Automatically

If your Macintosh has a modem, you can easily update the virus definitions file by using the UPDATE VIRUS DEFINITIONS... command.

To update new virus definitions automatically:

- 1 Choose UPDATE VIRUS DEFINITIONS... from the Tools menu.
The Update Virus Definitions dialog box appears (Figure 6-4).

Figure 6-4



- 2 The **Dial Phone Number** text box shows the phone number for accessing the virus definitions files.

The phone number is provided automatically during SAM installation. If the text box is blank or contains an incorrect phone number, see the SAM 4.5 Read Me file for the correct phone number. If you are outside of the U.S. or Canada, please contact your local dealer or Symantec office.

- 3 Select your modem type from the **Modem** pop-up menu.

If you do not know what kind of modem you have, the default selection will work in most cases. However, you may be able to speed up the file transfer by selecting the proper modem type.

- 4 Click Dial.

Messages appear on your screen to report the status of the file transfer.

NOTE: If the file transfer does not work with the default settings, see “Customizing Modem Settings,” on page 69.

After the file transfer is complete, the Updating Virus Definitions dialog box appears (Figure 6-5).

Figure 6-5

- 5 Click OK to return to the SAM Main Window.

Or,

Click Restart to restart your computer.

The new virus definitions are not in effect until you restart your computer.

TIP: You can schedule virus definition updates to occur at regular intervals. For more information, see [“Scheduling Virus Definition Updates,”](#) on page 54.

Unsuccessful File Transfer

If the file transfer didn't work, make sure you have the correct modem settings selected. See [“Customizing Modem Settings,”](#) on page 69, for more information.

If your modem settings are correct and the file transfer still doesn't work, make sure the modem is properly connected and turned on. Then refer to Appendix D, “System Messages.” If you cannot find an answer in these sections, refer to your modem's manual for help.

NOTE: If the file transfer was unsuccessful or otherwise aborted, the original virus definitions file is restored.

If the file transfer aborted because of a power outage, SAM will start with an error message. You must restore the virus definitions file before SAM can load. Look up the error message in [“System Messages,”](#) on page 121 for more information on how to resolve this problem.

Customizing Modem Settings

Although it is usually not necessary, there may be times when you need to change the modem settings in order for the file transfer to work.

To customize modem options:

- 1 Choose UPDATE VIRUS DEFINITIONS... from the Tools menu.
The Update Virus Definitions dialog box appears (see Figure 6-4).
- 2 Check **If Busy**, then specify in the **Redial *n* Times** and **Every *n* Seconds** text boxes how often SAM should redial if the phone line is busy.
The default settings are appropriate in most cases.
- 3 Select your modem type in the **Modem** pop-up menu.
If your modem is not in the list, select the generic option that most closely matches your modem (**Hayes-compatible**, **Generic V.32**, or **Generic MNP**). **Hayes-compatible** works in most situations.

TIP: You can speed up the file transfer by selecting the proper modem type.

- 4 Select the baud rate from the **Baud** pop-up menu. The fastest baud rate for your modem is selected automatically. You don't need to lower the baud rate unless the phone-line quality is impaired.
The file transfer will take a few minutes.
- 5 Select the dial type from the **Dial** pop-up menu (**Tone**, **Pulse**, or **Mixed**).
Tone is used for a touch-tone phone. **Pulse** is used for a rotary dial phone. **Mixed** dial type is used, for example, to dial out by pulse and then send a calling card number by tone.
- 6 Select one of the port icons shown to specify the port to which your modem is connected.
If you are not sure which port icon to select, look at the back of your Macintosh. The port to which your modem is connected will have an icon next to it that will match one of the icons in this dialog box.

NOTE: To update the virus definitions file, see “Updating Virus Definitions Automatically,” on page 66.

Updating Virus Definitions from a BBS

When a new virus definitions file becomes available, Symantec posts messages on several different bulletin board services. You can use any of these services to download a new virus definitions file.

NOTE: Each virus definitions file is dated. You can see the date of your current virus definitions file in the Virus Definitions dialog box. See “[Viewing the Virus List](#),” on page 63, for more information.

If the date of the SAM Virus Definitions file posted on the bulletin board system is newer than the date of the virus definitions file on your disk, download the new file.

To update the virus definitions file from a BBS:

- 1 Download the most recent virus definitions file from the appropriate BBS or the Internet.
See “[Accessing CompuServe and America Online](#),” on page 70, “[Accessing the Symantec BBS](#),” on page 71, and “[Updating Virus Definitions from the Internet](#),” on page 71, for information on how to access these services.
- 2 Move the new virus definitions file into your System folder.
The file must be named “SAM Virus Definitions” in order for SAM to use it.
- 3 Restart your computer so that the new virus definitions take effect.

Accessing CompuServe and America Online

Symantec maintains the Symantec Forums on CompuServe and America Online, where you can get updated virus definitions files.

To access the Symantec Forum on CompuServe:

- Type GO SYMMAC at any ! prompt.
The files are located in the SAM library.

To access the Symantec bulletin boards on America Online:

- 1 Choose Keyword from the Go To menu.
The Keyword dialog box appears.

- 2 Type SYMANTEC in the Enter Word(s) text box.
- 3 Click Go.

Check with CompuServe or America Online for data communications settings.

Accessing the Symantec BBS

Updated virus definitions files are available 24 hours a day on the Symantec Corporation bulletin board system (BBS). Settings for the Symantec bulletin board are: 8 data bits, 1 stop bit; no parity.

300- to 28,800-baud modems (541) 484-6669 (24 hrs.)

Updating Virus Definitions from the Internet

The current virus definitions files are located in the Symantec File Transfer Protocol (FTP) Internet site.

To use the FTP site:

- 1 Access `ftp.symantec.com`
- 2 The files are located in the `/public/AntiVirusDefs/sam/` directory.

To use the World Wide Web site:

- 1 Access `www.symantec.com`
- 2 Follow the on-screen directions.

Updating Virus Definitions from Disk

If you don't have a modem to download virus definitions automatically, you can get updated virus definitions files on disk. See "Getting Virus Definitions Update Disks," on page 72, for information on how to order update disks.

If you have already received the virus definitions update disk, follow the instructions in this section to update the file.

To install new virus definitions:

- 1 Insert the disk containing the updated virus definitions into the floppy drive.

The disk's window opens, showing the file icons on the disk.

2 Double-click the Installer icon.

If a SAM alert box appears asking if you want to suspend suspicious activity alerts during installation, click Yes.

The Easy Install dialog box appears.

3 Click Install.

If a SAM alert box appears telling you that installation cannot take place while other applications are running, either click Continue to close the other applications and continue installation, or click Cancel to exit the Installer.

When installation is complete, a dialog box appears indicating the installation was successful.

4 Click Restart.

Getting Virus Definitions Update Disks

You can order virus definitions update disks from Symantec to arrive by mail. This service requires a fee.

To order, do one of the following:

- In the United States, call (800) 453-1149.
- Outside the United States, contact your local Symantec office or representative.

Adding Virus Definitions Manually

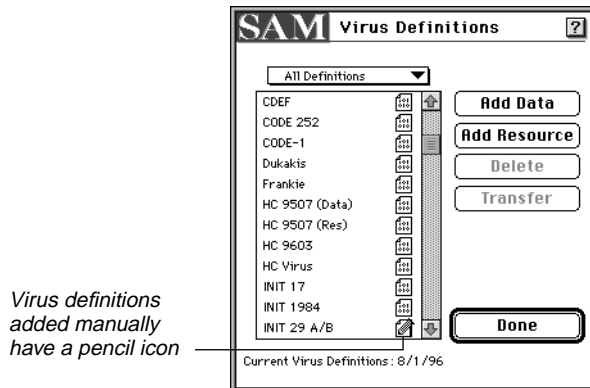
If you receive virus definition information from Symantec, use the procedure in this section to enter the new definition manually. The virus definitions you add manually allow SAM to detect new viruses, but not repair them. If a virus is detected, you must delete the file to remove the virus.

NOTE: If you download the latest virus definitions, you do not need to enter definitions manually—the new virus definition, along with all previous virus definitions, will already be in the virus definitions file. In fact, entering a duplicate virus definition may result in slower scanning and multiple reports for the same infection.

To add a virus definition manually:

- 1 Choose EDIT VIRUS DEFINITIONS... from the Tools menu.
The Virus Definitions dialog box appears (Figure 6-6).

Figure 6-6



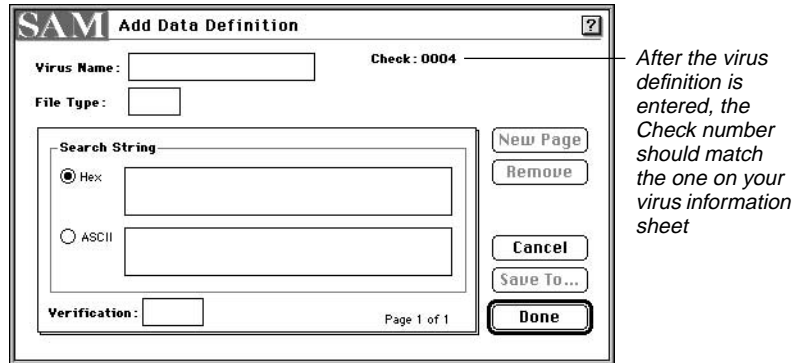
- 2 Look at the virus definition sheet sent to you to see which type of virus definition you are entering, then click either Add Resource or Add Data. (The diagram on the virus information sheet will look similar to either Figure 6-7 or 6-8.)

If you selected Add Resource, the Add Resource Definition dialog box appears (Figure 6-7).

Figure 6-7

If you selected Add Data, the Add Data Definition dialog box appears (Figure 6-8).

Figure 6-8



- 3 Enter the information exactly as it appears on the virus definition sheet.

Pay special attention to capitalization. Be sure to select the correct option buttons, too. If you are entering data in the **Hex** text box, you do not need to enter spaces.

NOTE: After the virus definition is entered, the Check number on the virus information sheet should match the Check number in the dialog box. If they do not match, recheck each entry carefully and correct as necessary.

- 4 If the virus definition has more than one page of information, click New Page to enter the additional information.
- 5 Click Done to save the virus definition.

Or,

If you want to save the virus definition to a User Definitions file on another disk, click Save To. The User Definitions file is in the Preferences folder.

The new virus definition will appear in the list with the pre-installed (called built-in) definitions (see Figure 6-6).

TIP: You can enter the virus definition once, then use the transfer feature to copy the virus definition to other computers that are using SAM. See “[Transferring Virus Definitions to Other Disks](#),” on page 76, for more information.

If You Can’t Save a Virus Definition

If a message appears preventing you from saving a definition, double-check your entries for accuracy and capitalization. SAM prevents you from saving an invalid definition.

If you get a message indicating the virus definitions file cannot be found, look in the System folder or the Preferences folder. The User Definitions file should be in the Preferences folder.

Deleting Virus Definitions

Occasionally you may need to delete a virus definition that was entered manually (when you’ve entered duplicate virus definitions, for example). Note that built-in virus definitions (those installed with SAM or from update disks or downloading) cannot be deleted.



Don’t delete a virus definition unless you are sure you don’t need it any more. Once a virus definition is deleted, SAM can’t detect the corresponding virus.

To delete a virus definition:

- 1 Choose EDIT VIRUS DEFINITIONS... from the Tools menu.
The Virus Definitions dialog box appears (see Figure 6-6).
- 2 Select **User Definitions** from the pop-up menu.
A list of virus definitions entered manually appears in the scrolling list.
- 3 Select the virus definition you want to delete.
- 4 Click Delete.
A dialog box appears asking you to verify the deletion.
- 5 Click Delete again.

Transferring Virus Definitions to Other Disks

When you enter a virus definition manually, there is no need to enter it for each computer that needs the new definition. Enter it once, then transfer the virus definition to the User Definitions files on other computers.

NOTE: You can only transfer virus definitions that you have entered manually.

To transfer a virus definition:

- 1 Choose EDIT VIRUS DEFINITIONS... from the Tools menu.
The Virus Definitions dialog box appears (see Figure 6-6).
- 2 Select **User Definitions** from the pop-up menu.
A list of manually entered virus definitions appears in the scrolling list.
- 3 Select the virus definition or definitions you want to transfer.
- 4 Click Transfer.
A directory dialog box appears.
- 5 Select the User Definitions file on the disk to which you want to transfer the virus definition.
The User Definitions file is in the Preferences folder.

Customizing SAM

7

This chapter explains how to customize SAM to fit your work environment.

Customizing Startup Options

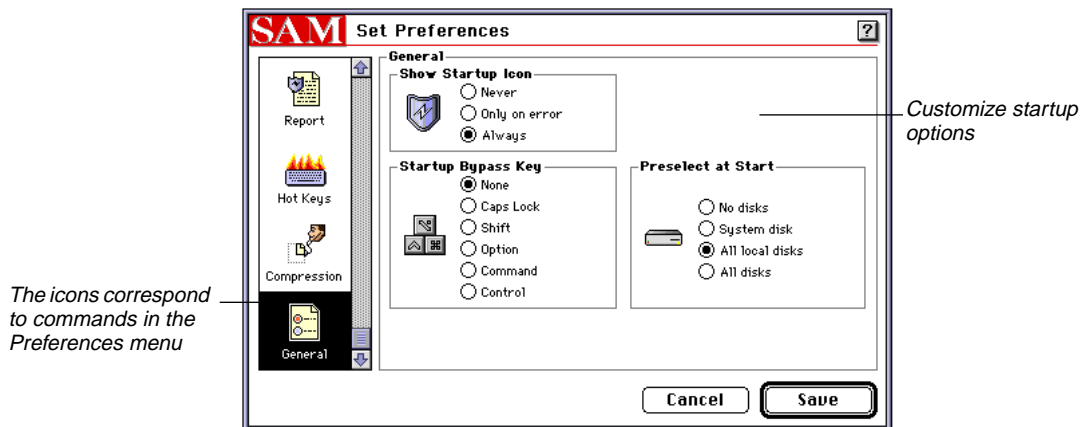
The startup options apply to SAM and SAM Intercept (the automatic protection feature of SAM that loads into memory when you start your computer.)

To customize startup options:

- 1 Choose GENERAL... from the Preferences menu.

The Set Preferences dialog box appears with the General options displayed (Figure 7-1).

Figure 7-1



- 2 Specify in the **Show Startup Icon** group box whether the SAM startup icon should appear each time your computer starts up.

The startup icon provides a visual cue that SAM Intercept is loading.

The **Only on error** option displays the startup icon with an "X" over it only if SAM Intercept cannot be loaded (for example, when your computer doesn't have enough memory to load SAM Intercept).

- 3 Specify in the **Startup Bypass Key** group box the key to hold down if you want to prevent SAM Intercept from loading when your computer starts up.

Select **None** if you don't want a bypass key available.

NOTE: Pressing Shift at startup prevents *all* system extensions from loading.

- 4 Specify in the **Preselect at Start** group box the disks that you want selected automatically in the SAM Main Window.

No disks: Does not preselect any disks when SAM is launched.

System disk: Preselects the startup disk.

All local disks: Preselects all disks not connected to a network.

All disks: Preselects all disks.

- 5 Click Save.

Or,

Proceed to the next section to continue customizing SAM.

Customizing Floppy Disk Scanning

The most common way for a virus to enter your computer is through floppy disks or other removable media. To prevent this from happening, SAM can automatically scan these items each time they are inserted into your computer.

To customize floppy disk scanning:

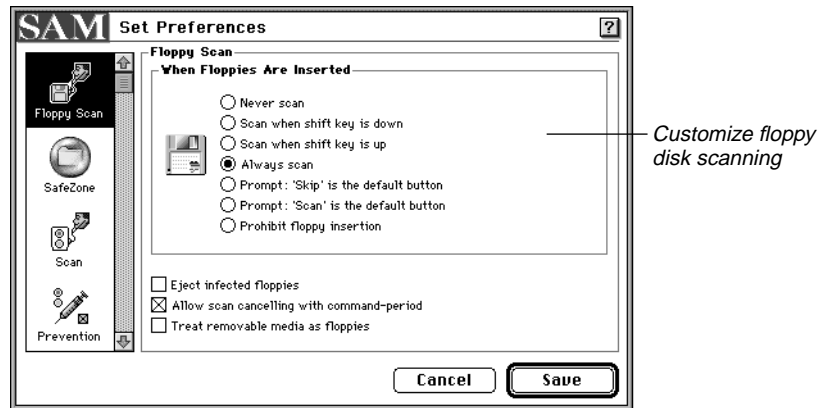
- 1 Choose FLOPPY SCAN... from the Preferences menu.

Or,

If the Set Preferences dialog box is already open, click the Floppy Scan icon.

The Set Preferences dialog box appears with the Floppy Scan options displayed (Figure 7-2).

Figure 7-2



- 2 Specify what SAM should do when a floppy disk is inserted.

Never scan: Does not automatically scan floppy disks for viruses.

Scan when shift key is down: Scans floppy disks only when the Shift key is pressed at the time of insertion.

Scan when shift key is up: Scans floppy disks when the Shift key is not pressed at the time of insertion. In this case, press Shift to skip the scan.

Always scan: Scans floppy disks each time they are inserted.

Prompt: 'Skip' is the default button: A dialog box will appear when floppy disks are inserted. The default button is Skip.

Prompt: 'Scan' is the default button: A dialog box will appear when floppy disks are inserted. The default button is Scan.

Prohibit floppy insertion: Ejects floppy disks. SAM will not allow access to floppy disks.

- 3 Check **Eject infected floppies** to prevent your computer from accessing an infected floppy disk.

NOTE: This option must be unchecked before you can repair an infected floppy disk.

- 4 Check **Allow scan cancelling with command-period** if you want to be able to stop an in-progress floppy disk scan. Pressing \mathcal{H} -. (Command-period) will stop the scan.

- 5 Check **Treat removable media as floppies** if you want all removable media, such as SyQuest cartridges, handled in the same manner as floppy disks.
 - 6 Click Save.
- Or,
- Proceed to the next section to continue customizing SAM.

Customizing Suspicious Activity Monitoring

A suspicious activity is an action that a virus might perform when damaging your files or spreading through your system. Although some applications perform these actions for valid reasons, SAM can monitor for these activities on the chance that an unknown virus is performing one of them.

If a suspicious activity is detected, it does not necessarily mean that a virus is performing the activity—you must decide whether to continue or not.

To customize suspicious activity monitoring:

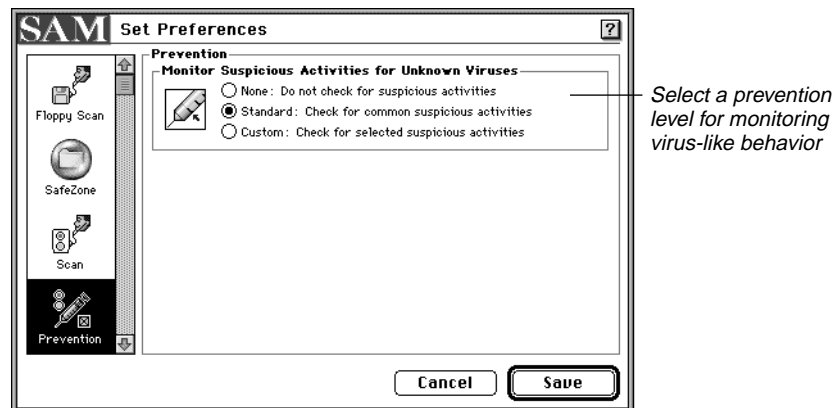
- 1 Choose PREVENTION... from the Preferences menu.

Or,

If the Set Preferences dialog box is already open, click the Prevention icon.

The Set Preferences dialog box appears with the Prevention options displayed (Figure 7-3).

Figure 7-3



- 2 Select a prevention level for monitoring suspicious activities.

None: Turns off suspicious activity monitoring.

Standard: Monitors applications for the most common virus behavior, such as adding code instructions to an application file.

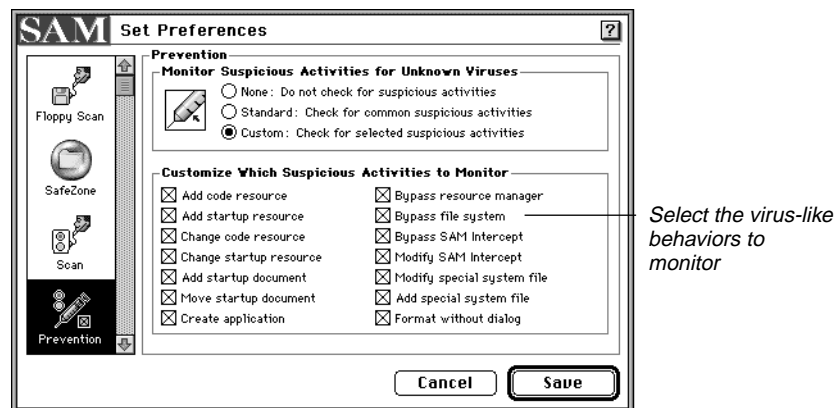
See step 3 for information on which activities are monitored in the Standard prevention level.

Custom: Lets you choose which suspicious activities SAM will monitor.

TIP: If you're not sure which option to choose, select **Standard**.

- 3 If you select **Custom**, an additional group of check boxes appears (Figure 7-4).

Figure 7-4



NOTE: Options with an asterisk (*) are included in the Standard prevention level.

***Add code resource:** A program tries to add code instructions to another file. This is the most common way viruses infect files. If this activity is detected, it is a good indication of an unknown virus at work.

Add startup resource: A program tries to add startup resource code to any file in the System folder. This is also a common way viruses infect. If this activity is detected, it is a good indication of an unknown virus at work.

***Change code resource:** A program tries to change a file's existing instructions. Programs rarely modify themselves. If this activity is detected, it is a good indication of an unknown virus at work.

Change startup resource: A program tries to change code resources in a startup document. If this activity is detected, it is a good indication of an unknown virus at work.

***Add startup document:** A program attempts to create a new startup document. Although this activity often happens legitimately (during the installation of new software, for instance), it could indicate an unknown virus at work.

Move startup document: A program tries to move a startup document into or out of the System folder. Although this activity often happens legitimately (when you move startup documents using the Finder, for example), it could indicate an unknown virus at work.

Create application: A program tries to create an application or a desk accessory file that can be started. Although this activity often happens legitimately (when you copy files using the Finder, for example), it could indicate an unknown virus at work.

Bypass resource manager: A program attempts to modify a resource file without going through the Macintosh Resource Manager. Modifications to a resource file are common; however, they normally take place using the facilities of the Resource Manager.

Although this activity often happens legitimately (when you use a backup program, for instance), it could indicate an unknown virus at work.

Bypass file system: A program attempts to modify a disk without going through the Macintosh file system. Although this activity could indicate an unknown virus at work, some applications (such as ResEdit, THINK C, and Macintosh Programmer's Workshop) bypass the file system as part of their normal processing.

***Bypass SAM Intercept:** A program attempts to modify a resource file without passing through checkpoints that SAM Intercept sets up for monitoring modification attempts.

This alert is fairly rare. If it appears, you should be suspicious because only a few programs (for example, THINK C, Pascal, and ResEdit) bypass SAM Intercept legitimately.

***Modify SAM Intercept:** A program attempts to make changes to SAM Intercept. If this activity is detected, it is a good indication of an unknown virus at work.

Modify special system file: A program attempts to write to the debugger, disassembler, or System file in a System folder. If this activity is detected, it is a good indication of an unknown virus at work.

Add special system file: A program attempts to move, rename, or create a debugger or disassembler file in a System folder. Attempts like this are infrequent and should be viewed suspiciously.

***Format without dialog:** A program attempts to format a disk without the standard format dialog box. This may be caused maliciously by a Trojan horse or legitimately by an application, such as a utility program attempting to create a disk partition. Attempts like this are infrequent and should be viewed suspiciously.

- 4 Click Save.

Or,

Proceed to the next section to continue customizing SAM.

Customizing Scanning Options

The scanning options you select apply to all scans—scans you initiate, scheduled scans, automatic floppy disk scans, and scans that take place automatically when you launch applications.

To modify scanning options:

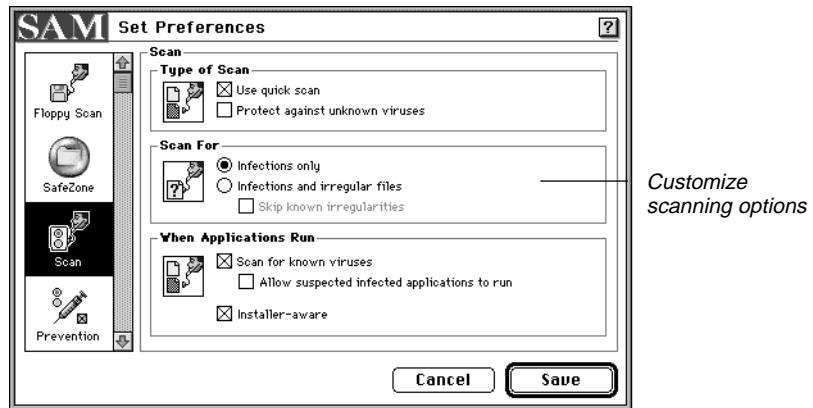
- 1 Choose SCAN... from the Preferences menu.

Or,

If the Set Preferences dialog box is already open, click the Scan icon.

The Set Preferences dialog box appears with the Scan options displayed (Figure 7-5).

Figure 7-5



- 2 Select scanning options in the **Type of Scan** group box.

Use quick scan: Scans all files for known viruses using the new quick scan technology.

Protect against unknown viruses: Monitors application files for changes that could indicate the presence of an unknown virus.

When SAM protects an application file, it records critical information about it (similar to taking a “fingerprint”). On subsequent scans, SAM checks the file against the “fingerprint” and notifies you if there are any changes that could indicate an unknown virus.

- 3 Specify the types of problems you want SAM to check for during a scan in the **Scan For** group box.

Infections only: Checks for known viruses.

Infections and irregular files: Checks for known viruses and irregularities in files that might indicate the work of an unknown virus.

Irregular files have characteristics that are “odd” or “abnormal.” Although irregularities reported in a file may indicate the presence of a virus, they do *not* necessarily mean the file is infected. Some programs legitimately have irregular characteristics.

Skip known irregularities: Does not report known irregularities of some common applications. (Some applications have irregularities that SAM knows about.)

NOTE: Checking for file irregularities does not apply to automatic floppy disk scans or automatic scans that occur when you launch an application.

- 4 Check **Scan for known viruses** to have SAM scan applications when they are launched.

If an application is infected, SAM will display an alert box allowing you to decide whether the application should continue launching.

- 5 Check **Allow suspected infected applications to run** if you want to choose whether to run an application even though it contains a virus. An alert box will allow you to choose whether to run the application or not.



Use caution when selecting this option. If you choose to run an infected application, the virus will activate and spread.

- 6 Check **Installer-aware** to suppress SAM alerts during installation of applications such as Norton Utilities for Macintosh, DiskDoubler, and other programs that use common installers.
- 7 Click Save.

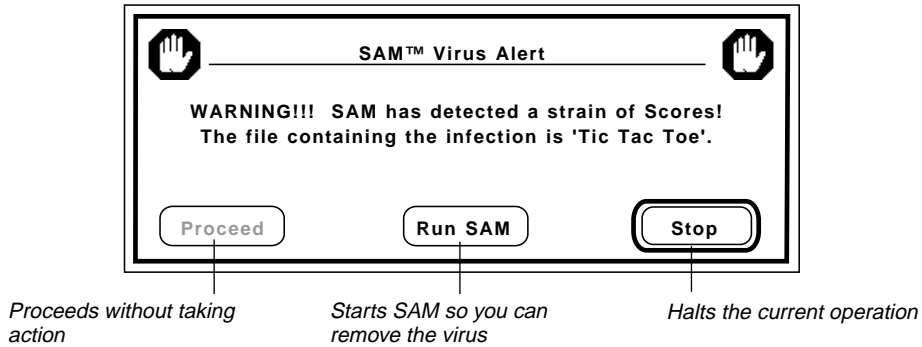
Or,

Proceed to the next section to continue customizing SAM.

Customizing Alerts

The alert settings specify how SAM informs you that it has detected a virus or suspicious activity. A suspicious activity is an action that viruses sometimes perform when damaging your files or spreading on your system. Figure 7-6 shows what a virus alert looks like.

Figure 7-6



To customize alerts:

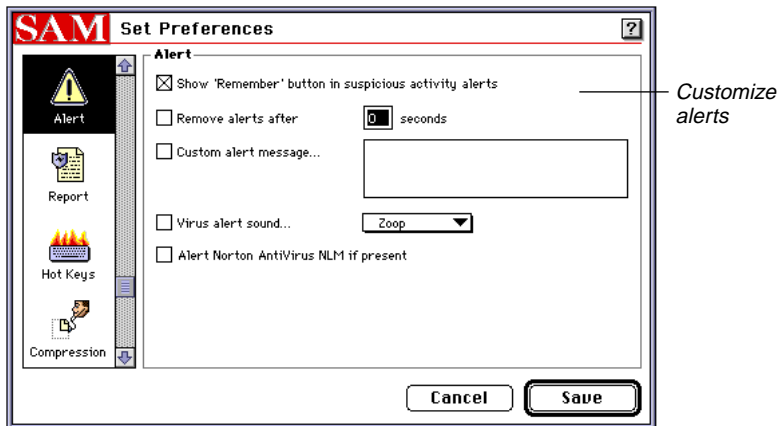
- 1 Choose ALERT... from the Preferences menu.

Or,

If the Set Preferences dialog box is already open, click the Alert icon.

The Set Preferences dialog box appears with the Alert options displayed (Figure 7-7).

Figure 7-7



- 2 Check **Show “Remember” button in suspicious activity alerts** if you want to allow SAM to ignore specific actions while a particular program is running.

Sometimes SAM alerts you of actions that could be the work of a virus, but in fact are not. In these cases, you can select the Remember button to add the file to the exceptions list, preventing the alert from appearing in the future. See “[Managing the Exceptions List](#),” on page 57, for more information.

- 3 Check **Remove alerts after** to specify how long alert boxes stay on your screen before the default button is selected automatically. Then enter the number of seconds (0 to 99) in the **seconds** text box.

For virus alerts the default button is always Stop. For suspicious activity alerts the default button is always Allow.

Or,

Uncheck this option if you want alerts to stay on the screen until you respond to them.

- 4 Check **Custom alert message** if you want a custom message to appear in virus alerts and suspicious activity alerts. Enter the message (such as “Call Lily for help”) in the text box.
- 5 Check **Virus alert sound** if you want to hear a sound when an alert appears on your screen. Select the sound from the pop-up menu.
The new sound will not take effect until you restart your computer.
- 6 Check **Alert Norton AntiVirus NLM if present** to have alerts from SAM sent to the Norton AntiVirus NetWare Loadable Module (NAVNLN) if it is present on your local network.

When NAVNLN receives such an alert, it will use its alert settings for real-time scans to determine who to notify and how to notify them. For more information, see the *Norton AntiVirus for NetWare User’s Guide*.

- 7 Click Save.

Or,

Proceed to the next section to continue customizing SAM.

Customizing Reporting Options

SAM generates two types of reports:

- Scan results that appear in the SAM Main Window.
- Scan results from automatic floppy disk scans, automatic scans when you launch an application, and suspicious activity alerts. These results are stored in the *Activity Log* file.

Customizing Scan Reports

You can specify whether to report on all files scanned or only those with problems (such as viruses and irregularities). You can also specify which application you will use to view the saved scan report files.

To customize reports:

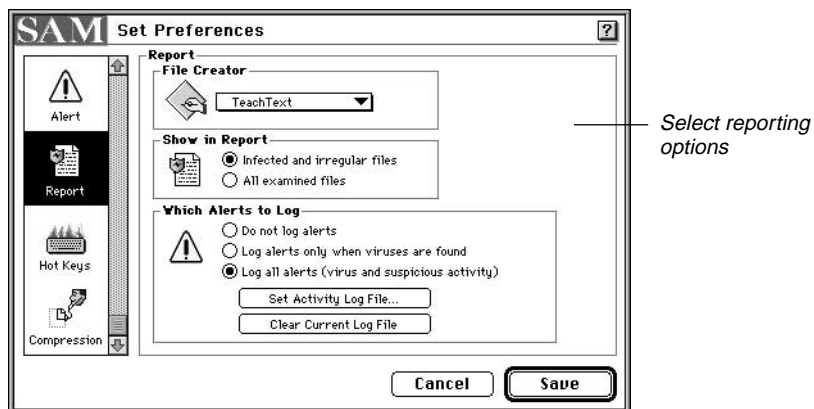
- 1 Choose REPORT... from the Preferences menu.

Or,

If the Set Preferences dialog box is already open, click the Report icon.

The Set Preferences dialog box appears with the Report options displayed (Figure 7-8).

Figure 7-8



- 2 Select an application from the **File Creator** pop-up menu. This allows you to view saved reports and the Activity Log in the application of your choice.

Choose **Other ()...** to select an application other than those listed. A dialog box appears that lets you locate the application.

- 3 Select an option in the **Show in Report** group box to specify the scope of reported information when scans are performed.

Infected and irregular files: Lists only files that contain known viruses and irregularities. This option minimizes the amount of information in the results list, making it easier to spot potential problems.

For information on irregular files, see “[Customizing Scanning Options](#),” on page 83.

All examined files: Lists every scanned file and reports whether a problem was found or not.

If problems are found, an alert will appear at the end of the scan.

Customizing the Activity Log

You can specify the name and location for the Activity Log and the types of alerts to record. You can also clear the Activity Log when it gets too big.

NOTE: The file format you chose in the File Creator group box also applies to the Activity Log.

To customize the Activity Log:

- 1 Select an option in the **Which Alerts to Log** group box to specify the type of alerts to save to the Activity Log (see Figure 7-8).

Do not log alerts: Does not log any information in the Activity Log file.

Log alerts only when viruses are found: Logs only virus warnings in the Activity Log file.

Log all alerts (virus and suspicious activity): Logs virus warnings and suspicious activity alerts in the Activity Log file.

Suspicious activities are actions that viruses sometimes perform. For more information, see “[Customizing Suspicious Activity Monitoring](#),” on page 80.

- 2 Click **Set Activity Log File...** to specify a location for the Activity Log file.

- 3 Click **Clear Current Log File** to clear the contents of the Activity Log file.
 - 4 Click Save.
- Or,
- Proceed to the next section to continue customizing SAM.

NOTE: To view the Activity Log, double-click the file.

Defining Hot Keys for Scanning

You can define up to ten special key combinations that you can press to begin scanning a file, folder, disk, or removable item (such as a floppy disk) without running SAM.

NOTE: SAM Intercept must be installed for the hot keys to work. If you performed an easy install, SAM Intercept is installed. If SAM Intercept is not installed, see [“Performing a Custom Install,”](#) on page 19.

To customize hot keys for initiating scans:

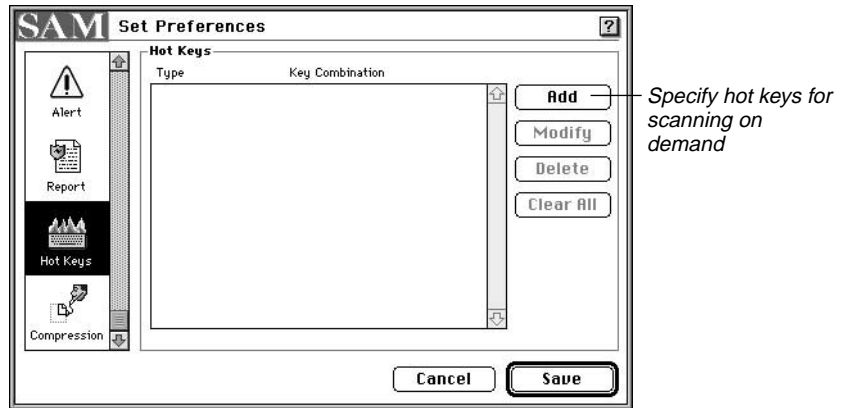
- 1 Choose HOT KEYS... from the Preferences menu.

Or,

If the Set Preferences dialog box is already open, click the Hot Keys icon.

The Set Preferences dialog box appears with the Hot Keys options displayed (Figure 7-9).

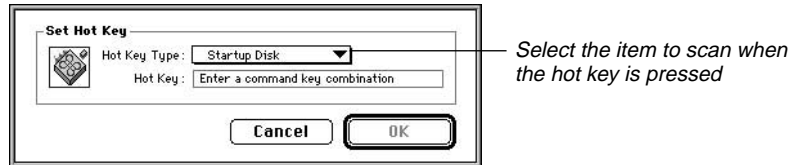
Figure 7-9



- 2 Click Add.

The Set Hot Key dialog box appears (Figure 7-10).

Figure 7-10



- 3 Select from the pop-up menu the item you want scanned when the hot key is pressed.

Startup Disk: Scans the startup disk.

Prompt: Lets you select a file, folder, or disk to scan.

Folder: Lets you select a folder to scan.

Disk: Lets you select a disk to scan.

Removable Media: Lets you select an internal floppy drive, external floppy drive, or other removable drive to scan.

- 4 Press the key combination you want to use. The hot key must include the Command (⌘) key. For example, Command-Shift-S.

The hot key will appear in the **Hot Key** text box.

TIP: Use an additional modifier key (such as Shift, Control, or Option) to reduce possible interference with a Command-key combination used by another application.

- 5 Click Save.

Or,

Proceed to “Selecting File Compression Options” later in this chapter to continue customizing SAM.

Modifying Hot Keys

If you ever need to change a hot key, it's easy to do.

To modify hot keys:

- 1 Choose HOT KEYS... from the Preferences menu.
The Set Preferences dialog box appears with the Hot Keys options displayed (see Figure 7-9).
- 2 Select the hot key to modify in the list box.
- 3 Click Modify.
The Set Hot Key dialog box appears (see Figure 7-10).
- 4 You can change the hot key type by selecting another option from the pop-up menu.
- 5 You can change the hot key by pressing a new key combination.
The hot key must include the Command key. For example, Command-Shift-S.
- 6 Click Save.

Deleting Hot Keys

You can delete one hot key at a time or delete all of them at once.

To delete hot keys:

- 1 Choose HOT KEYS... from the Preferences menu.
The Set Preferences dialog box appears with the list of hot keys displayed (see Figure 7-9).

- 2 Select the hot key to delete in the list box, then click Delete.
Or,
Click Clear All to delete all of the hot keys at one time.
- 3 Click Save.

Selecting File Compression Options

SAM can scan several different types of compressed files. SAM automatically scans all files compressed using AutoDoubler and SpaceSaver. In addition, you can specify which other compressed file types SAM should scan.

Note that compressed files are not scanned on automatic floppy disk scans.

To select which compressed file types to scan:

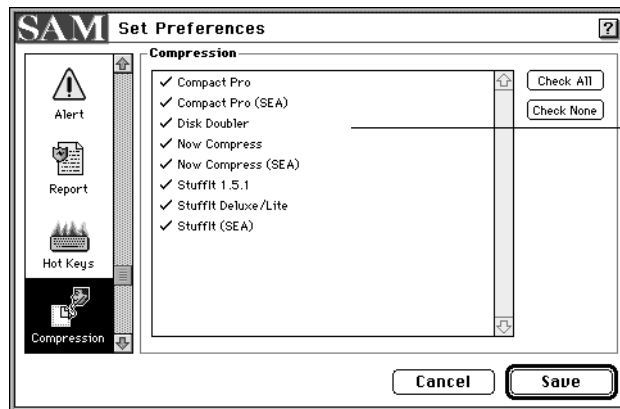
- 1 Choose COMPRESSION... from the Preferences menu.

Or,

If the Set Preferences dialog box is already open, click the Compression icon.

The Set Preferences dialog box appears with the Compression options displayed (Figure 7-11).

Figure 7-11



Select the file compression types that you want SAM to scan

- 2 Select the file compression types that you want SAM to scan. Click Check All to select all of the file types.

Or,

If you do not want compressed files scanned, click Check None.

NOTE: Scanning time may increase if you have many compressed files.

- 3 Click Save.

Specifying SafeZones

With more and more virus-infected files appearing on the Internet and Bulletin Board Systems (BBSs), you run the risk of infecting your Macintosh every time you download or receive a file. SafeZones are special locations on your disks that you use to receive downloaded files. To prevent virus infection, SAM immediately scans any file for viruses that is copied or downloaded to a folder designated a SafeZone.

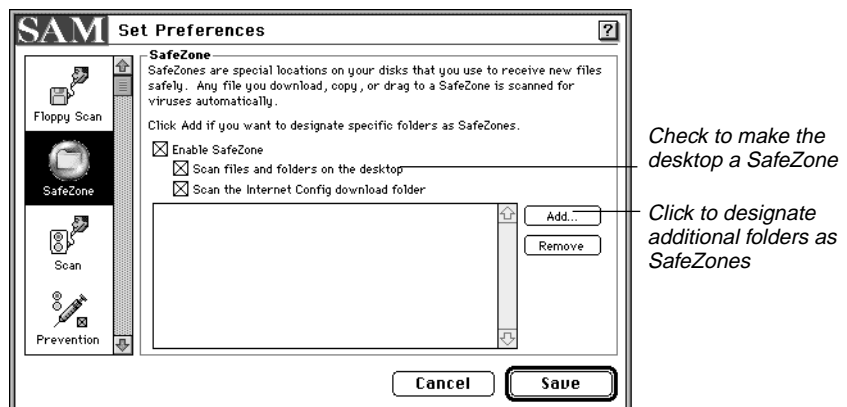
The preset SafeZone is your desktop. You can, however, designate any folders as SafeZones.

To specify a SafeZone:

- 1 Choose SAFEZONE... from the Preferences menu.

The Set Preferences dialog box appears with the SafeZone options displayed (see Figure 7-12).

Figure 7-12



- 2 Check **SafeZone Enabled** to make sure downloaded files are scanned for viruses.
- 3 Check **Scan Desktop Folders** if you want files copied or downloaded to the desktop scanned automatically.
- 4 If you use the Internet Config utility program, check **Scan Internet Config download folder**.

Internet Config is a popular Macintosh utility program to configure Internet browsers. With Internet Config, you designate a particular folder for all Internet downloads. If checked, SAM scans files arriving in this folder automatically.

- 5 Click Add... to specify additional folders as SafeZones.

Although it is generally more efficient to use just one or two folders for downloads, you can designate as many folders as SafeZones as are appropriate for your work habits.

- 6 Click Save.

Password-Protecting SAM

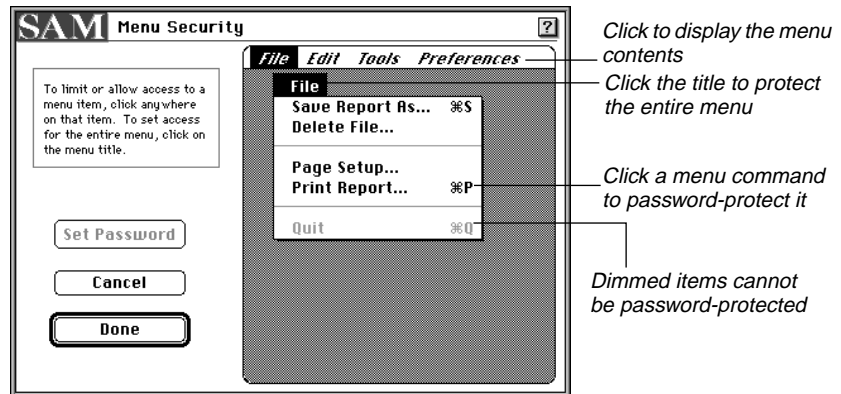
You can password-protect selected features of SAM to prevent others from changing your settings.

NOTE: Once you enter a password to access a password-protected feature, you can access all password-protected features without entering the password again.

To password-protect SAM features:

- 1 Choose MENU SECURITY... from the Preferences menu.
The Menu Security dialog box appears (Figure 7-13).

Figure 7-13



- 2 To password-protect a specific menu command, click the menu command.

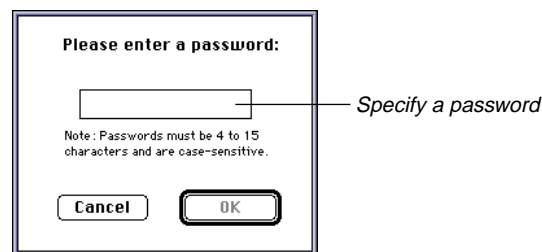
Or,

To password-protect an entire menu, click the menu title.

- 3 Click Set Password.

The set password dialog box appears (Figure 7-14).

Figure 7-14



- 4 Enter a password between 4 and 15 characters long (passwords are case-sensitive—for example, “a” is not the same as “A”), then click OK.

A dialog box appears prompting you to re-enter your password to validate it.

TIP: Write down your password and store it in a safe place.

5 Enter the password again, then click OK.

6 Click Done.

The protected features have a padlock icon next to them.

Changing Your Password

Once you've established a password, you can easily change it.

To change your password:

1 Choose MENU SECURITY... from the Preferences menu, then enter your password when prompted.

The Menu Security dialog box appears (see Figure 7-13).

2 Click Set Password.

The set password dialog box appears (see Figure 7-14).

3 Enter the new password, then click OK.

A dialog box appears prompting you to re-enter your password.

4 Enter the new password again, then click OK.

5 Click Done.

Removing Password Protection

If you decide you no longer want password-protection for some or all of the features you previously protected, you can easily remove the protection.

To remove password protection:

1 Choose MENU SECURITY... from the Preferences menu, then enter your password when prompted.

The Menu Security dialog box appears (see Figure 7-13).

2 Click the items that have a padlock icon next to them.

To unlock an entire menu, click the menu title.

The padlock icon disappears.

3 Click Done.

Menu Reference

8

This chapter provides a brief explanation of each SAM menu item.

File Menu

File	
Delete File...	
Save Report As...	⌘S
Page Setup...	
Print Report...	⌘P
Quit	⌘Q

Delete File...

DELETE FILE... displays a standard file dialog box where you can select a file to delete.

If the file you want to delete is shown in the scan results window, you can select the file and click the Delete button.

Save Report As...

SAVE REPORT AS... allows you to save SAM scan results to a file. A file dialog box appears with the default filename “SAM Report *date*” where *date* is the date of the scan.

The application that can open the file is determined by the Report File Creator selected in the REPORT command in the Preferences menu.

Page Setup...

PAGE SETUP... displays the standard Macintosh Page Setup dialog box where you can define the page layout before printing scan results.

Print Report...

PRINT REPORT... displays the standard Macintosh Print dialog box, allowing you to change the printing options before printing scan results.

Quit

QUIT exits from the SAM Main Window. You can also exit the SAM Main Window by pressing \mathbb{H} -Q (Command-Q). Note that QUIT does not affect SAM Intercept.

Edit Menu

Edit	
Undo	$\mathbb{H}Z$
Cut	$\mathbb{H}H$
Copy	$\mathbb{H}C$
Paste	$\mathbb{H}V$
Clear	
Select All	$\mathbb{H}A$

NOTE: The Edit menu is supported mainly for the use of desk accessories. Most of the commands are not available when using SAM.

Undo

UNDO is not available when using SAM.

Cut, Copy, and Paste

CUT, COPY, and PASTE are available when you are adding a password or custom alert message.

Clear

CLEAR erases the contents of the scan results list. CLEAR is available only when there is text in the scan results list and a desk accessory window is not open.

Select All

SELECT ALL selects all items in a list. For example, you can select all files in the scan results list or all disk icons in the SAM Main Window.

Tools Menu

Tools	
Scan & Protect	⌘L
Repair	⌘R
Scan & Eject	⌘E
Repair & Eject	
Scheduler...	
Edit Exceptions List...	
Edit Virus Definitions...	
Update Virus Definitions...	

Scan & Protect

SCAN & PROTECT checks files, folders, or disks to ensure that they are virus-free. Choosing SCAN & PROTECT is equivalent to selecting the Scan button in the SAM Main Window.

For more information, see [“Checking for Viruses,”](#) on page 31.

Repair

REPAIR scans files, folders, or disks for viruses and automatically repairs any viruses found.

For more information, see [“Repairing Infected Files,”](#) on page 42.

Scan & Eject

SCAN & EJECT lets you easily scan multiple floppy disks or other removable media.

For more information, see [“Scanning Multiple Floppy Disks,”](#) on page 35.

Repair & Eject

REPAIR & EJECT makes it easy and quick to repair multiple floppy disks or other removable media.

For more information, see [“Repairing Multiple Floppy Disks,”](#) on page 43.

Scheduler...

SCHEDULER... lets you set up scans to be performed at predetermined times. You specify what to scan and how often the scans should occur. If your computer has a modem, you can also schedule automatic virus definition updates at regular intervals.

For more information, see [“Scheduling Events,”](#) on page 52.

Edit Exceptions List...

EDIT EXCEPTIONS LIST... lets you print or remove entries from the Exceptions List. The Exceptions List contains normally suspicious conditions that you have told SAM to ignore when caused by a particular application or extension.

For more information, see [“Managing the Exceptions List,”](#) on page 57.

Edit Virus Definitions...

EDIT VIRUS DEFINITIONS... lets you add virus definitions manually from information provided by Symantec. You can also remove manually added virus definitions or transfer them to other computers.

Note that virus definitions you add manually allow SAM to detect new viruses, but not repair them. If a virus is detected, you must delete the file to remove the virus.

For more information, see [“Adding Virus Definitions Manually,”](#) on page 72.

Update Virus Definitions...

UPDATE VIRUS DEFINITIONS... lets you easily update the virus definitions file using your modem. If you have a modem, this is the most efficient way to update virus definitions.

Note that these virus definitions allow SAM to both detect and repair infected files.

For more information, see [“Updating Virus Definitions Automatically,”](#) on page 66.

Preferences Menu




Floppy Scan...

FLOPPY SCAN... lets you set floppy disk scanning options, such as whether to scan floppies automatically.

For more information, see [“Customizing Floppy Disk Scanning,”](#) on page 78.

SafeZone...

SAFEZONE... lets you specify which folders you use to receive Internet downloads and modem file transfers. All files are scanned for viruses immediately when they arrive in a SafeZone. The cursor changes to  while files are scanned.

For more information, see [“Specifying SafeZones,”](#) on page 94.

Scan...

SCAN... lets you customize options that apply to all scans, including scheduled scans, scans you initiate, and scans that SAM Intercept initiates automatically (when you launch an application, for example).

For more information, see [“Customizing Scanning Options,”](#) on page 83.

Prevention...

PREVENTION... lets you customize suspicious activity monitoring. A suspicious activity is an action that many viruses perform when damaging your files or spreading through your system.

For more information, see [“Customizing Suspicious Activity Monitoring,”](#) on page 80.

Alert...

ALERT... lets you customize the alert box that appears when a virus or suspicious activity is detected. A suspicious activity is an action that viruses sometimes perform when damaging files or spreading on your system.

For more information, see [“Customizing Alerts,”](#) on page 85.

Report...

REPORT... lets you customize SAM reports from scans that you initiate, scheduled scans that run automatically, and SAM Intercept scans that run when specific actions occur (when you launch an application, for example).

Hot Keys...

HOT KEYS... lets you define key combinations that you can press to scan a file, folder, disk, or removable item (such as a floppy disk) without opening the SAM Main Window.

For more information, see [“Defining Hot Keys for Scanning,”](#) on page 90.

Compression...

COMPRESSION... lets you specify which compressed file types SAM should scan. SAM automatically scans all files compressed using AutoDoubler and SpaceSaver.

For more information, see [“Selecting File Compression Options,”](#) on page 93.

General...

GENERAL... lets you customize startup options that apply to both SAM Intercept when it loads into memory at the time your computer starts up, and the SAM Main Window when you launch the SAM application.

For more information, see [“Customizing Startup Options,”](#) on page 77.

Menu Security...

MENU SECURITY... lets you password-protect selected features of SAM to prevent unauthorized access.

For more information, see [“Password-Protecting SAM,”](#) on page 95.

Turn Intercept Off

TURN INTERCEPT OFF lets you turn off SAM Intercept. Although we do not recommend doing this, it may be necessary at times (when troubleshooting INIT conflicts, for example).

When SAM Intercept is turned off, the option changes to TURN INTERCEPT ON.

About Computer Viruses



What Are Computer Viruses?

A computer virus is a parasitic program written intentionally to alter the way your computer operates without your permission or knowledge. A virus attaches copies of itself to other files, and when activated, may damage files, cause erratic system behavior, or merely display annoying messages.

What Viruses Do

Computer viruses infect executable files and documents created by applications with macro capabilities. These are Macintosh system files (including system extensions, INITs, and control panels), applications (such as word processing and spreadsheet programs), and document and template files (for example, created in Microsoft Word). A virus is inactive until you execute an infected application, start your computer from a disk that has infected system files, or open an infected document. Once a virus is active, it loads into your computer's memory and, at the very least, attaches copies of itself to applications, system files, and document and template files on disks you access.

Some viruses are programmed specifically to damage the data on your computer by corrupting programs, deleting files, or even erasing your entire hard disk. Many of the currently known Macintosh viruses, however, are not designed to do any damage. They simply replicate themselves and may display messages. However, because of bugs within the virus, your system may behave erratically or crash unexpectedly.

Even if you've never had a virus on your computer, you've probably heard of some of them. For example, the WDEF virus causes your computer to beep, frequently crash, or display fonts incorrectly. The nVIR virus beeps every 8 to 16 times you start your computer. One strain of the nVIR virus will generate the phrase "Don't panic" from your computer's speaker instead of beeping. Its designer probably found the idea amusing, but most victims do not.

What Viruses Don't Do

Computer viruses don't infect files on write-protected disks, and they usually don't infect documents. They don't infect compressed files either. However, applications *within* a compressed file could have been infected before they were compressed. Viruses also don't infect computer hardware, such as monitors or computer chips; they only infect software.

In addition, Macintosh viruses don't infect DOS-based computer software and vice versa. For example, the infamous Michelangelo virus does not infect Macintosh applications. Macro viruses, however, because they are attached to documents and templates that can be shared between Macintosh and DOS-based computers, can jump platforms. Your Word for Macintosh files can be infected by files created in Word for Windows.

Finally, viruses don't necessarily let you know that they are there—even after they do something destructive.

How Viruses Spread

Viruses spread when you launch an infected application, start your computer from a disk that has infected system files, or open an infected document. For example, if a word processing program contains a virus, the virus activates when you run the program. Once a virus is in memory, it usually infects any application you run, including network applications (if you have write access to network folders or disks).

Viruses behave in different ways. Some viruses stay active in memory until you turn off your computer. Other viruses stay active only as long as the infected application is running. Turning off your computer or exiting the application removes the virus from memory, but *does not* remove the virus from the infected file or disk. That is, if the virus resides in a system file, the virus will activate the next time you start your computer from the infected disk. If the virus resides in an application, the virus will activate again the next time you run the application.

To prevent virus-infected applications from getting onto your computer, scan files with SAM before you copy or run them. This includes applications you download from bulletin boards and any demo disks you receive.

About Trojan Horses

Trojan horses are not viruses; however, they are often thought of as viruses. A Trojan horse is a program that appears to serve some useful purpose or provide entertainment, which encourages you to run it. But, like the Trojan horse of old, it also serves a covert purpose which may be to damage files or perhaps plant a virus on your computer.

A Trojan horse is not a virus because it does not replicate and spread like a virus does. To ensure your safety, SAM will detect Trojan horses so that you can delete them from your computer.

About Worms

Worms are not viruses either. Worms are programs that replicate without infecting other programs. Some worms spread by copying themselves from disk to disk, while others replicate only in memory, creating myriad copies of themselves all running simultaneously, which slows down a computer.

Although worms exist in the realm of IBM-compatible personal computers, no occurrences of Macintosh worms have been reported—yet.

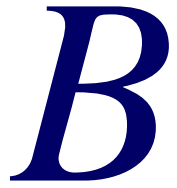
Getting More Information

For information on how to protect your system and avoid viruses, see “[Taking Precautions Against Viruses](#),” on page 51.

For information on a particular virus, see online help. For information on how to access this topic in online help, see “[Viewing Virus Descriptions](#),” on page 64.

For information on scanning for viruses, see “[Checking for Viruses](#),” on page 31.

Decontamination Procedures



If a virus has infected your Macintosh, you can use the *locked* Decontamination Disk you created to restart your Macintosh and remove the virus. If you don't have a Decontamination Disk, you can create one on another uninfected Macintosh. See “[Creating a Decontamination Disk](#),” on page 59, for instructions.

If your Macintosh starts up from the Apple Macintosh CD, you can start up your Macintosh from the CD, then you can use the SAM Install #2 disk to scan for viruses.

To start your Macintosh and remove a virus:

- 1 Shut down your Macintosh by choosing SHUTDOWN from the Special menu in Finder. Then insert your locked Decontamination Disk into the floppy drive and then restart your Macintosh.

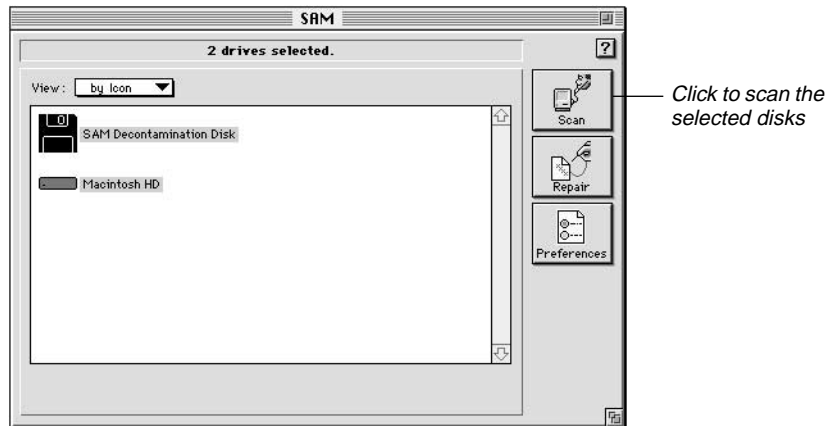
Or,

Restart your Macintosh from the Apple Macintosh CD if you have one. Then insert the SAM Install #2 disk into the floppy drive and double-click the SAM icon to start SAM. When prompted to find the virus definitions file, click Select to open the virus definitions file highlighted in the dialog box.

- 2 Type your name and organization when the personalization screen appears, then click OK.

The SAM Main Window appears (Figure B-1) with your hard disk already selected.

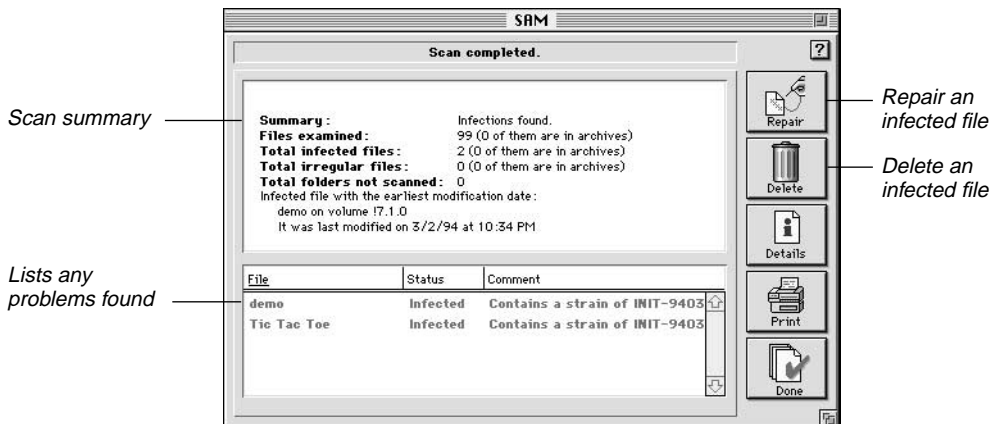
Figure B-1



3 Click Scan.

When the scan is complete, the results of the scan are shown in the scan results window (Figure B-2). The top portion of the screen shows a summary of the scan. The bottom portion of the screen lists any infected files.

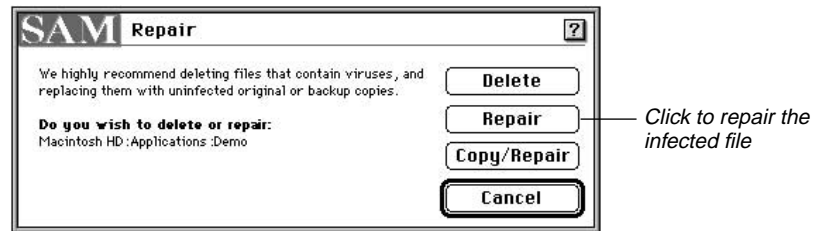
Figure B-2



4 If a virus was found, select the infected file or files in the scan results window, then click Repair.

To select more than one file, press Shift when you click the filename. A repair dialog box appears (Figure B-3).

Figure B-3



- 5 Click Repair again.

The Status column in the results list shows “Repaired” for the file.

NOTE: If SAM was not able to repair an infected file, see [“What to Do if Repair Is Unsuccessful,”](#) on page 44, for more information.

- 6 Click Done in the scan results window.
- 7 Choose QUIT from the File menu.
- 8 Restart your Macintosh.

Now that your hard disk is virus-free, scan all other floppy disks for viruses too. See [“Checking for Viruses,”](#) on page 31.

NOTE: If your Macintosh still does not start up properly after removing viruses, you may have to use a disk utility, such as Norton Utilities for the Macintosh or Disk First Aid, to resolve the disk problem.

Troubleshooting



This appendix explains how to resolve some common problems that may arise while you are using SAM. If the problem you are trying to resolve is not discussed in this appendix, see “[System Messages](#),” on page 121, and “[Taking Corrective Action](#),” on page 39, for more information.

Installation of SAM fails

- Restart your Macintosh with all extensions off (hold down the Shift key during the startup process). Then install SAM again.

NOTE: If you continue to have difficulty installing SAM, see “[General Macintosh Troubleshooting](#),” on page 117.

SAM Intercept fails to load when I start my Macintosh

- SAM Intercept may have a conflict with one or more of your other system extensions.

Check the SAM 4.5 Readme file for the most up-to-date information on compatibility with other system extensions. If the SAM 4.5 Readme file does not provide any answers, see “[General Macintosh Troubleshooting](#),” on page 117.

- If you are using an extension manager program, the program may have turned SAM Intercept off.

Launch the extension manager program and turn SAM Intercept back on if it has been turned off.

- Your copy of SAM Intercept could be damaged in some way. Reinstall SAM Intercept using the Custom install option. See “[Performing a Custom Install](#),” on page 19.

SAM cannot find the SAM User Definitions file

- The SAM User Definitions file should be in the Preferences folder. Use Find to locate the SAM User Definitions file, then move the file to the Preferences folder.

TIP: Look in the System folder first—you may find it there without the need to continue searching.

SAM cannot find the SAM Virus Definitions file

- The SAM Virus Definitions file must be located in the System folder. Use Find to locate the SAM Virus Definitions file, then move the file into the System folder.

SAM is automatically scanning my floppy disks more than once

- There is more than one copy of SAM Intercept or SAM Intercept Jr. in your System folder, Extensions folder, or Control Panels folder. Use Find to search for additional copies of SAM Intercept or SAM Intercept Jr., then remove the additional copies. You do not need to remove aliases of SAM Intercept or SAM Intercept Jr., since aliases only point to the actual copy.

SAM is reporting irregularities in my files

- Irregular files have characteristics that are “odd” or “abnormal.” Although irregularities reported in a file may indicate the presence of a virus, they do *not* necessarily mean the file is infected. Some programs legitimately have irregular characteristics.

For more information, see “[Resolving File Irregularities](#),” on page 44.

SAM is password-protected and I forgot my password

- If you forget your password, you must remove SAM from the SAM Folder and SAM Preferences from the Preferences folder. Then reinstall SAM to gain access to password-protected features.

For information on reinstalling SAM, see “[Performing a Custom Install](#),” on page 19.

How do I prevent SAM from loading first?

- Use an extension manager program to change the load order.
- You can change the location of SAM Intercept by moving it to the Control Panels folder or the System folder.
- Change the name of SAM Intercept.

During an automatic floppy scan, SAM did not scan every file on my disk

- A file on the disk may be damaged, or SAM ran out of memory, or some other error occurred during scanning.

Scan your disk again from the SAM Main Window. You may also want to examine the disk using the Norton Disk Doctor (part of the Norton Utilities for Macintosh).

Updating virus definitions via modem isn't working

- Make sure the modem is connected properly.
- Make sure you are using the correct modem cables.
- Make sure the modem is turned on.
- Verify that the modem settings are correct. See “Customizing Modem Settings,” on page 69, for more information.

See “System Messages,” on page 121, for information on specific error messages reported.

General Macintosh Troubleshooting

If you experience a problem starting your Macintosh after installing SAM, there may be a conflict with other extensions on your computer. Follow the procedures below to troubleshoot the problem.

Extensions may conflict for one or more of the following reasons:

- A file may be damaged.
- The files may need to be loaded in a different order.
- One of the files may need to be updated.

To identify multiple copies of system files:

- 9 Use Find to search for additional copies of the System file and the System folder.

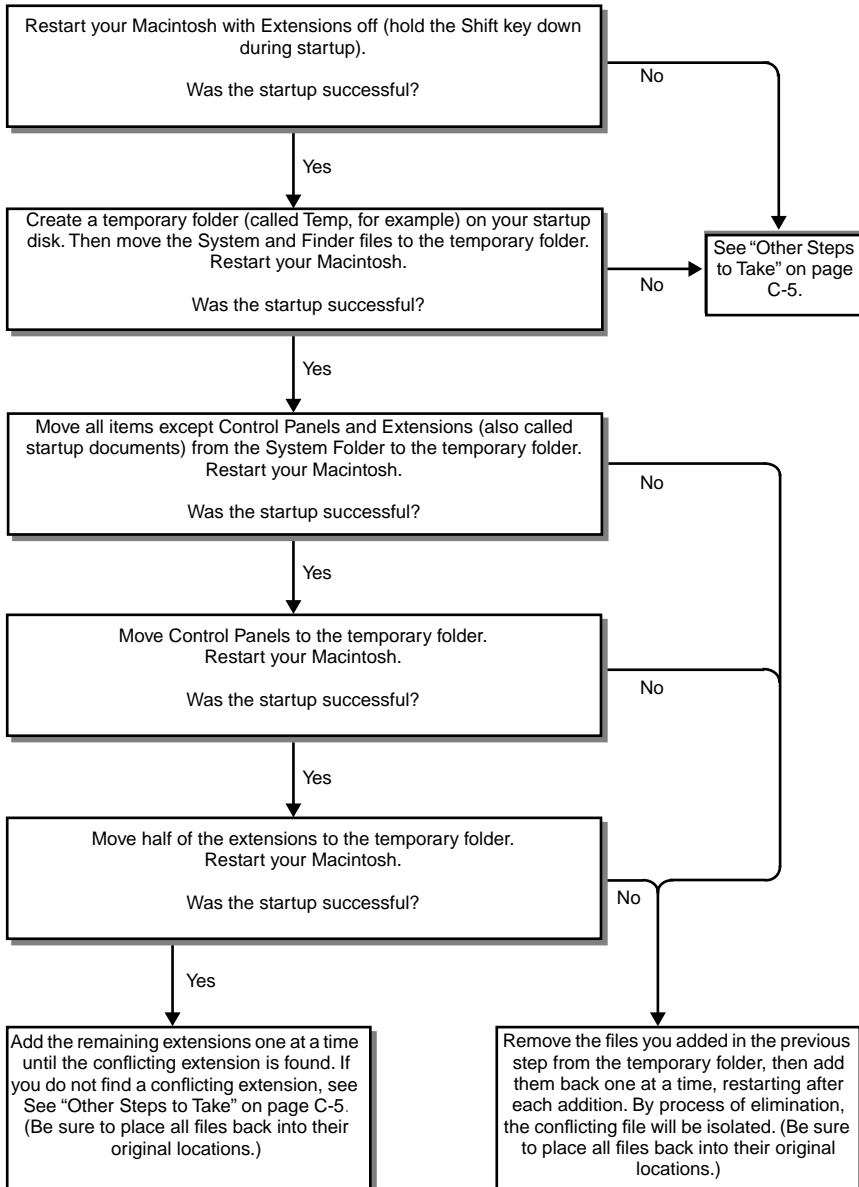
If there is more than one copy of the System file or the System folder, delete the additional copies.

- 10 Restart your Macintosh.

If the restart is successful, the problem is resolved.

If the restart fails, see the flowchart next.

To find an extension conflict:

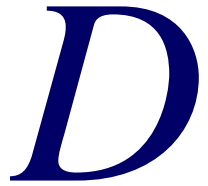


Other Steps to Take

Here are some other steps you can take to resolve problems with your Macintosh.

- Reinstall the System software.
See your Macintosh System documentation for more information.
- Use Norton Utilities for the Macintosh to find and fix disk problems.
- Rebuild the Desktop file.
See your Macintosh System documentation for more information.
- Reinstall SAM.
See “[Installing SAM](#),” on page 17, for more information.
- Update the disk driver.
See your Macintosh System documentation for more information.
- Reset the PRAM (Parameter RAM).
See your Macintosh System documentation for more information.

System Messages



This appendix contains an alphabetical list of the error messages you may encounter while using SAM.

A “System folder” scan was scheduled for a volume with no System file.

You scheduled a System folder scan for a disk that does not have a System file.

An error occurred during printing.

An unspecified error occurred during printing. Check the printer to make sure it is properly connected and turned on. Also make sure the printer is selected in Chooser.

An error occurred while attempting to open the selected file.

SAM encountered an error when trying to open a file. The file may be damaged, too many files may be open, or disk problems may have occurred.

An error occurred while copying this file.

SAM was not able to make a copy of the infected file. The file or disk may be locked or there may be insufficient disk space.

An error occurred while deleting this file.

SAM could not delete the file. The file or disk may be locked or no longer present.

An error occurred while dialing.

Make sure the phone line is connected properly and that the modem type is correct, then try again.

An error was encountered while trying to get information about that folder or disk.

The disk you are trying to access may be damaged or it may be a network disk that was disconnected.

Code 0 non-standard.

This message appears to alert you of some non-standard code in an application. It does not necessarily mean the file is infected with a virus. See [“Resolving File Irregularities,”](#) on page 44, for more information.

Code discontinuous & non-standard.

This message appears to alert you of some non-standard code in an application. It does not necessarily mean the file is infected with a virus. See [“Resolving File Irregularities,”](#) on page 44, for more information.

Files within archives cannot be repaired or deleted.

You must decompress the file before SAM can repair or delete it.

Help could not be opened.

This message appears when there is not enough memory to open the help file, the help file is damaged, or the help file cannot be found. You can increase SAM’s memory in the Get Info box in Finder. If increasing memory doesn’t solve the problem, reinstall SAM help. For more information, see [“Performing a Custom Install,”](#) on page 19.

Help could not be opened. The help file is already in use.

SAM is already open. You must exit one copy of SAM before the help file is available.

INIT in non-startup file.

This file contains a system extension (INIT), but the file is not a startup document. For more information see [“Resolving File Irregularities,”](#) on page 44.

Memory is very low. Unable to continue.

SAM needs more memory to complete the current operation. You can increase SAM's memory in the Get Info box in Finder.

Multiple INITs in file.

The startup document contains more than one system extension (INIT). Although some startup documents do contain multiple system extensions (for example, InterMail, AppleShare, and Easy Access), this is not common and could indicate the presence of a virus. You should check the original software to determine if this situation is normal. For more information see [“Resolving File Irregularities,”](#) on page 44.

No carrier was detected.

One or more of the modem settings are incorrect. Verify the modem type, baud rate, and phone number, then try again. See [“Customizing Modem Settings,”](#) on page 69.

No dial tone was detected.

The modem may not be connected to the phone line, or there is a problem with the phone line. Check the modem connection, then try again.

No files are selected.

You must select a file in the scan results list before clicking Repair, Delete, or Details.

No more data definitions may be added to this file.

The SAM User Definitions file already has the maximum number of data virus definitions, which is 64. You can delete definitions that are no longer needed. See [“Deleting Virus Definitions,”](#) on page 75, for more information.

No more details windows may be opened at this time.

The maximum number of details windows that can be opened at one time is 10.

No more resource definitions may be added to this file.

The SAM User Definitions file already has the maximum number of resource virus definitions, which is 64. You can delete a definition that is no longer needed. See “[Deleting Virus Definitions](#),” on page 75, for more information.

Not deleted - an unspecified error occurred.

SAM encountered an error while trying to delete a file, but the exact nature of the error is unknown. Restart your Macintosh, then delete the file.

Not deleted - the disk might be locked.

SAM cannot delete a file on a locked disk. To delete the file, you must first unlock the disk.

Not repaired - an unspecified error occurred.

SAM encountered an error while trying to repair a file, but the exact nature of the error is unknown. Delete the infected file, then replace it with an uninfected backup copy. For more information, see “[Deleting Infected Files](#),” on page 41.

Not repaired - file is already open.

SAM cannot repair a file that is currently open and in use. Restart your computer using your Decontamination Disk, then scan and repair the file. See “[Decontamination Procedures](#),” on page 111, for more information.

Not repaired - the disk might be locked.

You are trying to repair a file on a locked disk. To repair the file, you must first unlock the disk.

Not repaired - the infection is non-standard.

SAM does not have the information to repair this file. This can happen if the file has been damaged beyond repair. To remove the virus, you must delete the file. For more information, see “[Deleting Infected Files](#),” on page 41.

One or more errors occurred while processing Apple Events.

SAM could not continue because an error occurred. SAM may not have enough memory, or the file SAM is trying to scan may be damaged.

One or more resources are missing from SAM. Please reinstall SAM from the original disks.

The SAM application file is damaged. Reinstall SAM from the original disks.

Problems occurred during this repair.

SAM encountered some type of error when attempting to repair a file. The virus may have damaged the file beyond repair, or the file or disk may be locked.

Problems were found during the scan.

SAM found an infected file or an irregularity while scanning your files. The scan results list shows the details of what was found. See [“Taking Corrective Action,”](#) on page 39, for information on how to resolve these problems.

SAM has been modified (possibly by a virus). Please reinstall SAM from the original disks.

The SAM files have changed in some way. Reinstall SAM from the original disks. For more information, see [“Performing an Easy Install,”](#) on page 17.

SAM requires System 7.0 or later to run.

SAM runs only under System 7.0 or later.

SAM will not run on this machine.

You are trying to run SAM on an incompatible machine (such as Macintosh 128, 512, or 512e).

Startup document is invisible.

This system extension has been assigned an attribute making it invisible, so it does not appear on your desktop. System extensions should never be made invisible, so this change may be caused by a virus. See [“Resolving File Irregularities,”](#) on page 44, for more information.

Text was too long. The string was truncated to 100 characters.

You attempted to paste more than 100 characters into a custom alert message.

That is not a valid Macintosh disk.

The disk you inserted to scan is not a Macintosh disk.

That key is already used as a hot key. Please select a different key.

The hot key combination you selected is already in use. You must choose another key combination.

That password is incorrect.

You entered an incorrect password. If you forgot your password, see “[Troubleshooting](#),” on page 115, for more information.

The “Event Type” option has been changed to “Scan System disk” because only the System disk or folder can be scanned at startup.

The startup scan you scheduled can only scan the System folder or the entire system disk.

The “How often” option has been changed to “weekly” because “always” can only be used with startup or shutdown scans.

When you change the type of scan from startup or shutdown to some other type, the frequency must also change if it was set to “always.” The “always” setting only applies to startup and shutdown scans.

The “When” option has been changed to “at specified time” because virus definition updates cannot be scheduled at startup or shutdown.

Virus definition updates cannot occur at startup or shutdown. You must specify a different time for the update to occur.

The Communications Toolbox has not been installed properly. Please reinstall the Communications Toolbox from the original SAM disks.

The Communications Toolbox was not installed properly. You can install it using the custom install feature. For more information, see “[Performing a Custom Install](#),” on page 19.

The definition may be incomplete or entered incorrectly.

The virus definition was not entered correctly. Double-check your entries for accuracy and capitalization. SAM prevents you from saving an invalid definition.

The Desktop file contains code of type *type*.

SAM found what appears to be code in a desktop file. The code resource type is specified in *type*. Because this situation should not occur, scan this file immediately.

The initialization command was not accepted by the modem; please recheck the modem type in the configuration dialog.

The wrong modem type is selected in the Update Virus Definitions dialog box. Change the modem type, then try again. See “[Customizing Modem Settings](#),” on page 69.

The line appears to have been dropped.

Phone line noise probably caused the connection to fail. Try again.

The line was busy.

Check the “If Busy Redial” option in the Update Virus Definitions dialog box, then specify how often SAM should redial if the phone line is busy. See “[Customizing Modem Settings](#),” on page 69.

The modem is not responding. Please make sure the cables are plugged in, the modem is on, and the correct speed has been selected.

The wrong modem type or baud rate is selected in the Update Virus Definitions dialog box, or the modem is not properly connected. Check the modem connection and verify the correct modem type and baud rate, then try again. See “[Customizing Modem Settings](#),” on page 69.

The number was either invalid or too large. It was changed to a valid number.

The number you pasted into the “Remove alerts after x seconds” was invalid or too large. The number cannot be larger than 99.

The passwords did not match. Please try again.

The second password you entered does not match the first one.

The remote system did not answer.

The phone number may be incorrect. See the SAM 4.0 Readme file for the correct phone number.

The SAM Activity Log cannot be saved to a network disk. Please select a different location.

You can only save the Activity Log to a local disk.

The SAM Virus Definitions file is invalid.

You must replace the SAM Virus Definitions file because it was either tampered with or damaged in some way. See “[Adding New Virus Definitions](#),” on page 66, for more information on getting a new virus definitions file.

The selected user definitions cannot be added to this file. They would exceed the maximum allowed.

The SAM User Definitions file cannot store more than 128 virus definitions (64 resource definitions and 64 data definitions). To make room, you can delete a virus definition that is no longer needed. See “[Deleting Virus Definitions](#),” on page 75, for more information.

The selected user virus definitions were successfully deleted. The built-in definitions cannot be deleted.

The built-in virus definitions you selected cannot be deleted. Only user virus definitions can be deleted.

The selected user virus definitions were successfully transferred. The built-in definitions cannot be transferred.

The built-in virus definitions you selected cannot be transferred to another SAM User Definitions file. Only user virus definitions can be transferred.

There is not enough memory to open that folder or disk.

SAM does not have enough memory to display the contents of the folder or disk. You can increase SAM's memory in the Get Info box in Finder.

There was a problem opening the data fork.

The file is probably damaged. Replace the file with a backup copy.

There was a problem scanning the data fork.

The file is probably damaged. Replace the file with a backup copy.

This file contains <virus name> resources (type).

This file contains the same resource type as a known virus. The code resource type is specified in type. You should contact the software manufacturer to find out if the resource type is valid. If it is not supposed to be present, delete the file and replace it with an uninfected copy.

This file is probably not a valid resource file.

SAM encountered an error when trying to open a resource file. This usually indicates that the resource fork is invalid or damaged. Delete the file, then replace the file with a copy from the original disk.

The virus was removed, but the file must be replaced.

SAM was able to successfully remove the virus, but the file was irreparably damaged and must be replaced. Delete the file, then replace it with an uninfected copy from the original disk.

This virus infection cannot be repaired.

SAM does not have the information needed to repair this file. The virus definition was entered manually into the User Definitions file, which cannot be used to repair viruses; or the virus has caused irreparable damage. To remove the virus you can delete the file and replace it with an uninfected copy. For more information, see “[Deleting Infected Files](#),” on page 41.

Timed out while attempting to establish connection.

The phone number may be incorrect. See the SAM 4.5 Readme file for the correct phone number.

Unable to add this virus definition.

SAM was not able to add the virus definition to the SAM User Definitions file. The file or disk may be locked or there may be insufficient disk space.

Unable to clear the Activity Log.

Disk errors occurred when SAM tried to delete the Activity Log file. The file or disk may be locked.

Unable to create or open the User Definitions file.

SAM encountered a problem while attempting to open the SAM User Definitions file. The file or disk may be locked or disk space may be insufficient.

Unable to delete the selected virus definitions.

SAM encountered a disk or file error while attempting to delete a virus definition. The file or disk may be locked.

Unable to examine this file - it is already open.

SAM cannot scan a file that is currently open and in use. You must close the file before scanning it.

Unable to find exceptions.

SAM cannot find the SAM Preferences file or the file is damaged. If the Preferences file is damaged, you must delete it so that SAM can create a new one.

Unable to find or open the SAM Virus Definitions file. Make sure it is located in the System folder.

SAM could not find the virus definitions file in the System folder. If you are not able to locate this file, see [“Adding New Virus Definitions,”](#) on page 66, for information on getting a new virus definitions file.

Unable to locate this file.

SAM cannot locate the target file. The file has been deleted, moved, or renamed.

Unable to read all the code in this file.

SAM encountered a resource error while reading the code from the resource file. This message may appear if the code resources are extremely large. Try increasing the amount of memory allocated to SAM in the Finder Get Info box.

Unable to transfer the selected virus definitions.

SAM was not able to transfer the virus definitions to the SAM User Definitions file you selected. The file or disk may be locked.

Unable to unlock the selected file.

SAM was unable to unlock the specified file while attempting to add, delete, or transfer virus definitions. This message may appear if you have a security program that keeps the file locked.

Unable to update exceptions.

SAM cannot update exceptions because the SAM Preferences file is damaged or there is insufficient disk space. If the file is damaged, you must delete it so that SAM can create a new one.

Unable to write to the report file.

SAM was not able to save the report file to the specified location, possibly because of a locked disk or lack of disk space.

You cannot open that folder or disk until at least one open folder has been closed.

There is not enough memory for SAM to display any more files. Close an open folder you no longer need.

You do not have sufficient access privileges to open that folder.

The folder you are trying to scan is probably on a network drive where you don't have access privileges.

You don't need to enter spaces, since they are added for you as needed.

The virus definition you are entering uses hexadecimal numbers. Virus definitions of this type do not require you to enter spaces.

Your SAM Preferences file is invalid or could not be created. Delete your existing SAM Preferences file and try again.

You are trying to run SAM with a damaged Preferences file. Delete the SAM Preferences file, then launch SAM again.

Your scheduled event will not occur until SAM Intercept is installed.

SAM Intercept must be installed before scheduled scans can run. For information on installing SAM Intercept, see ["Performing a Custom Install,"](#) on page 19.

Using SAM on a Network



You can run SAM on any AppleTalk Transaction Protocol server, such as AppleShare or TOPS. This appendix offers tips and suggestions for using SAM efficiently on a network.

TIP: You can install SAM on workstations over an AppleTalk network using the SAM Administrator. This program is included with multi-user packs and site licenses of SAM software.

Notes to the Administrator

We recommend setting up SAM the following way in a networking environment:

- Run SAM Intercept and the SAM Main Window on the system administrator's computer.
- At the very least, make sure SAM Intercept is run on all workstation Macintosh computers.
- Use the SCHEDULER... command from the SAM Tools menu to schedule periodic scans of all network drives.

Scanning Network Drives

When you are scanning network drives from a workstation, the server slows down for other users. If others are creating, deleting, or moving files on a network drive while SAM is scanning, all files may not get scanned. To prevent this, you can do the following:

- Make sure you are the only one logged on to the server when scanning network drives.

Or,

- Shut down the server and restart it as a workstation. Then perform the scan.

NOTE: The SAM Main Window cannot run on an AppleShare volume at the same time as AppleShare (version 2.x).

Using SAM Intercept on a Server

To protect against viruses, we strongly recommend using SAM Intercept on your server or servers. SAM Intercept will monitor file activity and alert you if a virus tries to infect any applications on the server.

If you are using the Prevention feature to monitor suspicious activities, you may experience delays because SAM Intercept constantly monitors the Macintosh on which it is installed.

To prevent a network slowdown when using Prevention:

- 1 Select the **Standard** prevention level in Prevention options.

The **Standard** option monitors applications for the most common virus behavior, such as adding code instructions to an application file.

For more information, see “[Customizing Suspicious Activity Monitoring](#),” on page 80.

- 2 Check **Remove alerts after** in the Alert options. Then, type 0 in the **seconds** text box.

This will prevent suspicious activity alerts from halting access to files on the server by automatically accepting the default button in the alert box.

For more information see, “[Customizing Alerts](#),” on page 85.

- 3 Select **Log all alerts (virus and suspicious activity)** in the Report options.

This will ensure that suspicious activity alerts are logged in the Activity Log file so you can view the alerts at a later time.

For more information, see “[Customizing Reporting Options](#),” on page 88.

Preparing an Emergency Response Plan

To be fully prepared in case of a virus attack on a workstation, be sure to have a detailed emergency response plan written and distributed within your networking group before a problem arises. This will maintain order and prevent panic in case of an infection.

The following sections include a partial listing of the items that should be contained in your plan. You will, of course, want to complete your plan based on the dynamics and needs of your organization.

Before a Virus Is Detected

Conduct an informational meeting with your network users to discuss the basic nature and behavior of computer viruses. Stress that while having a computer virus on your system is reason to take immediate action, there is no need to panic. Emphasize that many viruses spread from illegal or “bootlegged” software copies, and prohibit the use of such software in your organization. Finally, explain how you’ve configured SAM to respond to a virus.

TIP: You can add a customized message to all virus alerts and suspicious activity alerts to indicate who the user should call for help (for example, “Call Lee for help at x2345”). For more information, see [“Customizing Alerts,”](#) on page 85.

Instruct your users to:

- Scan all software before using it. This includes programs downloaded from electronic bulletin boards as well as new software right out of the shrink-wrapped box.
- Watch for warning signs such as frequent system crashes, lost data, screen interference, or suddenly unreliable programs.
- Keep a current store of virus-free program backups.
- Avoid running programs from floppy disks they haven’t scanned.
- Write-protect their floppy disks before using them in someone else’s computer.

To protect the workstations:

- Scan each workstation to make sure it is virus-free.
- Create and write-protect a decontamination disk for each workstation and store it in a safe place.
- Train your users to use a file backup utility on a regular basis.
- Train your users to update the virus definitions file when it becomes available. If you are using SAM Administrator, the virus definitions files on workstations can be updated automatically.

To protect the network:

- Password-protect all network executable directories so that only you (the administrator) have write access to them.
- Scan for viruses on new and rental computers before using them.
- Schedule periodic scans of all network servers.
- If you are using a Novell NetWare server, use Norton AntiVirus for NetWare to protect the server from virus infections.

If a Virus is Detected

- Physically disconnect the workstation from the network. Then eradicate the virus on the workstation before reconnecting to the network.
- Notify other users on the network to scan for viruses immediately.
- Scan your network servers for viruses.

Glossary

alert box	A dialog box that appears on your screen to notify you that a virus or suspicious activity has been detected. You must respond by clicking a button or pressing Return.
alias	A representative object that points to an original object (file, folder, or disk). Aliases give you quick access to applications, files, folders, and disks without having to seek out the originals. An alias looks like its original counterpart except the name appears in <i>italics</i> .
AppleShare	An extension that lets you access shared files on other networked Macintosh computers or AppleShare file servers.
AppleTalk	A network communications environment (developed by Apple Computer) in which many different kinds of computers, related hardware (peripherals), and software can work together.
application	A computer program written for a specific purpose, such as word processing or creating a spreadsheet. Also called program or application program.
archive file	A single file or group of files that have been compressed into one file. <i>See also</i> “compressed file,” on page 138.
ASCII	American Standard Code for Information Interchange (pronounced “ASK-ee”). A standard that assigns a unique binary number (a byte) to each text character and control character.
baud rate	The speed at which a modem can transmit data. Baud rate measures the number of signal changes that occur in one second. “Baud rate” and “bps” are not synonymous.
(to) boot	To start a computer.
bps	(bits per second). A measure of speed in serial transmission. Also used to describe hardware capabilities (i.e., a 9600-bps modem). The term “bps” is not the same as “baud rate.”
built-in virus definition	<i>See</i> “SAM Virus Definitions file,” on page 142.
bulletin board system (BBS)	An on-line service that allows messaging, electronic mail, and file transfer between computer users via modem.

compressed file	A file that has been compressed using a special data storage format to save space on your disk. <i>See also</i> “ archive file ,” on page 137.
(file) creator code	A four-character sequence associated with a file that specifies which application created the file.
data definition	A definition for viruses that attack data files (more accurately, the data fork of a file), such as HyperCard stacks.
data fork	The part of a Macintosh file that contains data. For example, text entered using a word processor is stored in the data fork of the document file. <i>See also</i> “ resource fork ,” on page 141.
default button	A button with a heavy border that activates when you click it or press Enter.
desk accessory	A “mini-application” that is available from the Apple menu regardless of which application you are currently using.
desktop	Your working environment on the computer—the gray area below the menu bar (the default desktop pattern is gray). The Finder puts icons for each mounted disk on the desktop, along with the Trash icon.
desktop file	An invisible file used by the Finder to store information such as the location of file and folder icons on a disk.
dialog box	A window that appears on your screen, containing buttons, check boxes, etc.
directory	<i>See</i> “ folder ,” on page 139.
disk	A storage device. There are two main types: floppy disks and hard disks. A disk is sometimes referred to as a volume. <i>See also</i> “ partition ,” on page 140.
document file	A file that is created by or associated with an application and contains no executable code. Examples include word processing documents, databases, and spreadsheets.
download	To transfer a file from one computer system to another, usually through a modem. Usually refers to the act of transferring a file from a bulletin board system (BBS) such as CompuServe or America Online.

encryption	A way to impose data security on selected files, folders, or disks. Encryption disguises data. Often the encrypted item is protected with a password so that only those knowing the password can access (decrypt and use) the data.
Exceptions List	Group of normally suspicious conditions that you have told SAM not to look for in a particular file. Exceptions are saved when you click the Remember button in a suspicious activity alert.
executable file	A file containing program code that can be launched. Generally includes any file that is an application, extension, or a system file.
extension	See “ system extension ,” on page 142.
file server	A central disk storage device (or devices) connected to a network that provides network users access to shared applications and data files.
file system	An operating system mechanism that governs the definition of a file and how files are created, stored, updated, and deleted.
file type	A four-character code, stored along with a creator code in each file, that identifies its type. Applications use this code to determine if a file is in a format that can be read by the application.
folder	A grouping of files and/or folders that is represented by a folder-shaped icon on the desktop. Folders can contain documents, applications, and other folders. A folder is sometimes referred to as a directory or subdirectory.
Hayes-compatible	Responding to the same commands as a modem manufactured by Hayes Microcomputer Products, originators of the standard for microcomputer modems.
hexadecimal (hex)	The representation of numbers in base-16, using the digits 0 through 9 and letters A through F. Hexadecimal numbers are used when manually entering some virus definitions.
icon	A graphic symbol used to represent a file, folder, disk or other entity.
INIT	See “ system extension ,” on page 142.
infected file	A file that contains a virus.

irregular file	An application that is not constructed in accordance with the standards set for Macintosh applications. Sometimes this is intentional; other times it is the sign of a virus. Irregularities are not necessarily the result of viruses, but should be investigated.
known virus	Any virus that SAM can detect and identify by name.
LAN (Local Area Network)	A group of computers connected for the purpose of sharing resources. The computers on a local area network are typically joined by a single transmission cable and are located within a small "local" area such as a single building or section of a building.
launch	To start or run an application.
load	<i>See "launch".</i>
locked disk	<i>See "write-protected disk," on page 143.</i>
locked file	A file that can be viewed, but cannot be written to or deleted. Also referred to as read-only.
MNP	(Microcom Networking Protocol). A series of error control and data compression protocols used by some modems.
modifier key	A key that can be pressed in sequence with an alphanumeric character to execute a command instead of printing the character to the screen. The standard modifier keys are Caps Lock, Command, Control, Option, and Shift.
mount	To make a Macintosh disk available for use on the desktop. When a disk is mounted, its icon appears on the desktop.
MultiFinder	A multi-tasking operating system component that allows more than one application to be open at the same time, performing background tasks while you perform other tasks.
network	A set of computers and associated hardware (printers and so forth) connected together in a work group for the purpose of sharing information and hardware among users.
operating system	A program that ties the capabilities of computer hardware and software to input/output devices such as disks, keyboards, and mice.
partition	A portion of a disk (prepared and set aside by a special disk utility) that functions as a separate disk. When partitions are mounted to the desktop, a separate icon appears for each partition.

program	See “ application ,” on page 137.
protection	A SAM feature that generates information about a file that can be used to verify the file’s integrity. This feature helps protect against unknown viruses.
read-only	A disk, folder, or file containing data that can be read, but cannot be written to or deleted. Also referred to as locked or write-protected.
removable media	Disks that can be removed, as opposed to hard disks that are stationary. Some examples of removable media are floppy disks, disk cartridges (SyQuest and Bernoulli, for example), and CDs (Compact Discs).
repair	To remove a virus from a file and return the file to its original, uninfected state.
resource fork	The part of a file that contains information used by an application, such as menus, fonts, icons, and the executable code. Most viruses attach themselves to the resource fork of application files.
resource manager	The portion of Macintosh system software through which an application accesses various resources, such as icons, fonts, and menus.
restart	To start your computer again. You can do this by choosing RESTART from the Special menu of the Finder, or by turning your Macintosh on after you have shut it down.
scan	The systematic search for viruses performed by SAM.
SAM Intercept	The automatic protection feature of SAM that loads into memory at startup to guard your computer against viruses.
SAM Intercept Jr.	The automatic protection feature in SAM that works the same as SAM Intercept, but does not monitor for suspicious activities. It takes less memory than SAM Intercept and cannot be customized.
SAM User Definitions file	A file that contains virus definitions entered from information provided by Symantec. SAM uses these virus definitions to detect viruses, but not repair them. If a virus is detected, you must delete the file to remove the virus. See also “ SAM Virus Definitions file ,” on page 142.

SAM Virus Definitions file	A file that comes with the SAM software package and provides information for finding and repairing viruses. Also called built-in definitions. You can download a new virus definitions file from Symantec BBS, CompuServe, Applelink, and America Online bulletin board services.
shut down	To turn off your Macintosh or prepare it to be turned off.
startup	The process by which your computer starts working. During this process, system extensions such as SAM Intercept are loaded into memory.
startup disk	A disk (hard disk or floppy disk) with all the necessary program files—such as the Finder and System files contained in the System folder—to set a Macintosh into operation. Sometimes called a boot disk or system disk.
suspicious activity	An activity or action caused by other software that SAM perceives as the work of a possible unknown virus. Suspicious activity alerts do not necessarily indicate the presence of a virus, but should be investigated.
system extension	A program that loads into memory when a Macintosh is started. Also known as a startup document. In System 6, a system extension is called an INIT file.
System file	A file stored in the System folder that the Macintosh uses to start up.
System folder	A folder on the startup disk that contains the files your Macintosh requires for operation, such as the System file, Finder, system extensions, desk accessories, and control panels.
Trojan horse	A program that promises to be something useful or interesting (like a game), but may covertly damage or erase files on your computer while you are running it. Trojan horses are not actually viruses because they do not replicate or spread to other files.
unknown virus	A virus for which SAM does not contain a virus definition. <i>See also</i> “virus definition,” on page 143.
user definitions	<i>See</i> “SAM User Definitions file,” on page 141.

virus	A self-replicating program written intentionally to alter the way your computer operates without your permission or knowledge. A virus attaches copies of itself to other files, and when activated, may damage files, cause erratic system behavior, or merely display annoying messages.
virus definition	Virus information that allows SAM to recognize and alert you to the presence of a specific virus. <i>See also</i> “ SAM User Definitions file ,” on page 141, and “ SAM Virus Definitions file ,” on page 142.
volume	<i>See</i> “ disk ,” on page 138.
worm	A program that replicates without infecting other programs. Some worms spread by copying themselves from disk to disk, while others replicate only in memory to slow down a computer. So far, worms do not exist in the Macintosh world.
write-protected disk	A disk that cannot be written to or erased. Write-protecting disks prevents viruses from infecting them. To write-protect a 3.5-inch disk, slide the tab on the back of the disk to uncover the hole through the disk. Also referred to as a “locked disk” or “read-only disk.”

Symantec Service and Support Solutions

Symantec is committed to excellent service worldwide. Our goal is to provide you with professional assistance in the use of our software and services, wherever you are located.

Technical Support and Customer Service solutions vary by country. If you have questions about the services described below, please refer to the section "Worldwide Service and Support" at the end of this chapter.

Registering your Symantec product

To register your Symantec product, please complete the registration card included with your package and drop the card in the mail. You can also register via modem during the installation process (if your software offers this feature) or via fax to (800) 800-1438 or (541) 984-8020.

Technical Support

Symantec offers several technical support options designed for your individual needs to help you get the most out of your software investment.

Symantec *StandardCare Support* is available at no charge to all registered users of Symantec software. This support option offers 90 days of telephone technical support (from the date of your first call), and is designed for customers who need assistance getting started with their new software.

StandardCare Support is available Monday through Friday, 7:00 a.m. to 4:00 p.m. Pacific Time. See the back of this manual for the support telephone number for your product.

For more information on Symantec Support Solutions, including PriorityCare and PremiumCare Support, please call our automated fax retrieval service, located in the United States, at (800) 554-4403 or (541) 984-2490, and request document 070. Alternatively, visit Symantec on the World Wide Web at:

<http://www.symantec.com>

Online support

Technical support is also available through several online services 24 hours a day. All registered Symantec customers have unlimited access to this information.

World Wide Web and FTP

Point your Web browser to:

<http://www.symantec.com/techsupp>

to find the latest Frequently Asked Questions (FAQs), search the Symantec Knowledge Base for solutions to common situations, or post your own query to a support newsgroup. All messages posted to the discussion group receive a response from a Symantec representative (posted back to the discussion group) within 48 hours. These forums are in Usenet newsgroup (Internet news) format and require a newsreader.

You can also FTP directly to this site to download technical notes and software patches at:

<ftp://ftp.symantec.com>

CompuServe and America Online

Exchange information and ideas with Symantec representatives and other users of Symantec products in the Symantec forums on CompuServe (GO SYMANTEC) and America Online (Keyword: SYMANTEC).

All messages posted to CompuServe and America Online receive a response from a Symantec representative within 48 hours.

For additional information, data communications settings, or to subscribe to these services, call:

America Online	U.S. and Canada	(800) 227-6364
CompuServe	U.S. and Canada	(800) 848-8199
	All Other Locations	+1 (614) 718-2800

Symantec Bulletin Board Service (BBS)

The Symantec BBS provides a customer service forum, shareware and public domain software, FAQs, file download service, and access to our Internet discussion groups. Set your modem to 8 data bits, 1 stop bit, no parity and dial (541) 484-6669.

Automated fax retrieval system

You can use Symantec's automated fax retrieval system 24 hours a day to receive product information directly to your fax machine.

For general product information, fact sheets and product upgrade order forms, please call our Customer Service fax retrieval system at (800) 554-4403 or (541) 984-2490.

For technical application notes, please call our Technical Support fax retrieval system on (541) 984-2490 and select option 2.

Support for old and discontinued versions

When a new version of this software is released, registered users will receive upgrade information in the mail. Telephone support will be provided for the previous version for 6 months after the release of the new version. Technical information may still be available through Online Support.

When Symantec announces that a product will no longer be marketed or sold, telephone support will be discontinued 60 days later. Support will only be available for discontinued products through online services. See the section "Online Support" previously in this chapter.

Customer Service

Symantec's Customer Service department can assist you with non-technical questions. Call Customer Service to:

- Order an upgrade.
- Subscribe to the Symantec Support Solution of your choice.
- Fulfill your request for product literature or demonstration disks.
- Find out about dealers and consultants in your area.

- Replace missing or defective CDs, disks, manuals, etc.
- Update your product registration with address or name changes.

You can also visit Customer Service online at:

<http://www.symantec.com/custserv>

for the latest Customer Service FAQs, to find out the status of your order or return, or to post a query to a Customer Service discussion group.

Customer Service discussion groups provide a forum for customers to ask general questions about Symantec products and services. All messages posted receive a response from a Symantec customer service representative within 2 business days. These forums are in Usenet newsgroup (Internet news) format and require a newsreader.

Worldwide Service and Support

Symantec provides Technical Support and Customer Service worldwide. Services vary by country and include International Partners who represent Symantec in regions without a Symantec office.

Service and Support offices

NORTH AMERICA

Symantec Corporation	(800) 441-7234 (USA & Canada)
175 W. Broadway	(541) 334-6054 (all other locations)
Eugene, OR, 97401	Fax: (541) 984-8020

Automated Fax Retrieval	(800) 554-4403
	(541) 984-2490

EUROPE

Symantec Europe Ltd.	+31 (71) 535 3111
Kanaalpark 145	Fax: +31 (71) 535 3150
2321 JV Leiden	
The Netherlands	

Automated Fax Retrieval	+31 (71) 535 3255
-------------------------	-------------------

ASIA/PACIFIC RIM

Symantec Australia Pty. Ltd. +61 (2) 9850 1000
408 Victoria Road Fax: +61 (2) 9850 1001
Gladesville, NSW 2111
Australia

Automated Fax Retrieval +61 (2) 9817 4550

Most International Partners provide Customer Service and Technical Support for Symantec products in your local language. For more information on other Symantec and International Partner locations, please call our Technical Support automated fax retrieval service, in the United States at +1 (541) 984-2490, choose Option 2, and request document 1400.

Every effort has been made to ensure the accuracy of this information. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change without prior notice.

Symantec AntiVirus for Macintosh™

Disk Exchange and/or Replacement Form

DISK EXCHANGE: Symantec AntiVirus for Macintosh is available on 800K low-density disks. If you have purchased a product that does not contain the correct disk size for your computer, you may exchange the disks at no extra charge. Simply fill out Section A, enclose all original disks, and mail to the address below.

DISK REPLACEMENT: After your 60-Day Limited Warranty, if your disk(s) becomes unusable, fill out Sections A & B and return 1) this form, 2) your damaged disks, and 3) your payment (see pricing below, add sales tax if applicable), to the address below to receive replacement disks. *DURING THE 60-DAY LIMITED WARRANTY PERIOD, THIS SERVICE IS FREE.* You must be a registered customer in order to receive disk replacements.

SECTION A - FOR DISK EXCHANGE AND REPLACEMENT

Please send me: ☐ 800K low-density disks (exchange only) ☐ 1.44M high-density disks (exchange or replacement)

Name

Company Name

Street Address (No P.O. Boxes, Please)

City State Zip/Postal Code

Country* Daytime Phone

Software Purchase Date

*This offer limited to U.S., Canada, and Mexico. Outside North America, contact your local Symantec office or distributor.

SECTION B - FOR DISK REPLACEMENT ONLY

Briefly describe the problem:

Disk Replacement Price \$ 10.00
Sales Tax (See Table) \$ 4.95
Shipping & Handling \$ 4.95
TOTAL DUE

SALES TAX TABLE: AZ (5%), CA (7.25%), CO (3%), CT (6%), DC (5.75%), FL (6%), GA (4%), IA (5%), IL (6.25%), IN (5%), KS (4.9%), LA (4%), MA (5%), MD (5%), ME (6%), MI (6%), MN (6.5%), MO (4.225%), NC (6%), NJ (6%), NY (4%), OH (5%), OK (4.5%), PA (6%), SC (5%), TN (6%), TX (6.25%), VA (4.5%), WA (6.5%), WI (5%). Please add local sales tax (as well as state sales tax) in AZ, CA, FL, GA, NY, OH, OK, SC, TN, TX, WA, WI.

FORM OF PAYMENT ** (Check One):

☐ Check (Payable to Symantec) Amount Enclosed \$ ☐ Visa ☐ Mastercard ☐ American Express

Credit Card Number Expires

Name on Card (please print) Signature

****U.S. Dollars. Payment must be made in U.S. dollars drawn on a U.S. bank.**

MAIL YOUR DISK EXCHANGE AND/OR DISK REPLACEMENT ORDER TO:

Symantec Corporation
Attention: Order Processing
175 West Broadway
Eugene, OR 97401-3003

Please allow 2-3 weeks for delivery within the U.S.

Symantec and Symantec AntiVirus for Macintosh are trademarks of Symantec Corporation.
Other brands and products are trademarks of their respective holder/s.
© 1997 Symantec Corporation. All rights reserved. Printed in the U.S.A.

Index

A

- Activity Log, 89
- Add Data Definition dialog box, 74
- Add Resource Definition dialog box, 73
- ALERT... command, 86, 104
- alerts
 - customizing messages in, 85–87
 - removing, 87
 - responding to
 - file changed alert, 48
 - suspicious activity alert, 47
 - virus alert, 39–40
 - sending to Norton AntiVirus NLM, 87
 - suspending during software installation, 85
- Allow command button, 47
- America Online, 70
- Apple Installer, awareness in SAM, 85
- AppleShare, 133
- AppleTalk, 133
- application renaming, 57
- application, infected. *See* infected application
- Audit Trail. *See* Activity Log
- AutoDoubler files, 93
- automatic protection. *See* SAM Intercept
- automatic scanning, 94
- avoiding virus infections, 51

B

- background, scanning in, 23
- backup files, 42, 43
- Balloon Help, 30
- BBS
 - scanning files from, 94
 - updating virus definitions from, 70
- beep, on alert, 87

- boot. *See* startup
- built-in virus definition, 63
- bulletin board services. *See* BBS
- bypass key, 78
- bypassing SAM Intercept at startup, 78

C

- Cancel icon, 32
- cartridges, removable. *See* removable media
- checking for viruses. *See* scanning
- checksum. *See* fingerprint of files
- CLEAR command, 100
- commands
 - ALERT..., 104
 - CLEAR, 100
 - COMPRESSION..., 104
 - COPY, 100
 - CUT, 100
 - DELETE FILE..., 99
 - EDIT EXCEPTIONS..., 102
 - EDIT VIRUS DEFINITIONS..., 102
 - FLOPPY SCAN..., 103
 - GENERAL..., 105
 - HOT KEYS..., 104
 - MENU SECURITY..., 105
 - PAGE SETUP..., 99
 - PASTE, 100
 - PREVENTION..., 104
 - PRINT REPORT..., 99
 - QUIT, 100
 - REPAIR, 101
 - REPAIR & EJECT, 101
 - REPORT..., 104
 - SAFEZONE..., 94
 - SAVE REPORT AS..., 99
 - SCAN..., 103
 - SCAN & EJECT, 101

commands (*continued*)

- SCAN & PROTECT, 101
- SCHEDULER..., 102
- SELECT ALL, 100
- TURN INTERCEPT OFF, 105
- UNDO, 100
- UPDATE VIRUS DEFINITIONS..., 102
- Compact Pro files, 93
- comprehensive scan. *See* Quick scan option
- compressed files, 31
 - scanning, 93–94
 - virus infections in, 108
- COMPRESSION... command, 93, 104
- CompuServe, 70
- computer virus. *See* virus
- Continue icon, 32
- conventions of this manual, 15
- COPY command, 100
- copying virus definitions, 76
- customizing
 - Activity Log, 89
 - alert options, 85–87
 - file compression options, 93–94
 - floppy disk scanning, 78–80
 - hot keys for scanning, 90–92
 - installation, 19–21
 - message in alerts, 87
 - modem settings, 69
 - password protection, 95–97
 - prevention options, 80–83
 - reports, 88
 - SafeZone folders, 94
 - scanning options, 83–85
 - scheduled virus scans, 55
 - startup options, 77–78
 - suspicious activity monitoring, 80–83
- CUT command, 100

D

- data definition, 74
- date of virus definitions files, 64

Decontamination Disk

- creating, 59
- updating, 61
- using, 111
- write-protecting, 61
- definitions files. *See* virus definitions files
- DELETE FILE... command, 99
- Delete icon, 32
- deleting
 - hot keys, 92
 - infected files, 41
 - password, 97
 - scheduled virus scans, 55
 - virus definitions, 75
- Deny command button, 48
- details
 - about files, 46
 - about viruses, 64
- Details icon, 32, 46
- dialog box options, 15
- disabling SAM Intercept, 28
- Disk Doubler files, 93
- disks
 - ejecting infected floppy disks, 79
 - infected, 43
 - infected. *See* infected application
 - preselecting at SAM startup, 78
 - repairing multiple floppy disks, 43–44
 - scanning for viruses, 31–33
 - automatically, 79
 - multiple floppy disks, 35
 - network disks, 133
 - scheduling scans of, 53
 - using to update virus definitions, 71
 - viewing contents of, 34
 - write-protected, 108
- Done icon, 32
- downloading virus definitions, 66–69
- drives. *See* disks

E

- EDIT EXCEPTIONS... command, 102
- Edit menu, 100

EDIT VIRUS DEFINITIONS... command, 102

editing

Edit menu commands for, 100

Exceptions List, 57

See also customizing

Eject command button, 40

eliminating viruses from files, 40–44

emergency response plan, network, 134–136

encrypted files, 31

error messages. *See* system messages

Exceptions List

editing, 57

of acceptable suspicious activities, 57–59

printing, 58

warning about renaming applications, 57

exiting SAM, 27, 100

extension conflicts, resolving, 117

F

file changed alert, 48

file irregularities

resolving, 44–46

scanning for, 84

skipping in scan, 84

File menu, 99

file server, using SAM on, 133–136

file system modifications, 82

files

backup, 42

compressed, 31, 93–94, 108

deleting, 41

details about, 46

encrypted, 31

fingerprints of, 56

infected, 40

irregular, 44–46, 84

protecting against unknown viruses,
56–57

repairing, 42–44

unsuccessful, 44

replacing with uninfected copies, 41

saving reports to, 37, 99

scanning, 33

downloaded, automatically, 94

files (*continued*)

selecting, 34

viewing details, 46–47

virus definitions. *See* virus definitions files

fingerprint of files, 56

floppy disks

automatic scanning, 78–80

customizing scan options, 78–80

multiple, repair of, 43–44

preventing access to infected, 79

scanning, 35

See also disks

FLOPPY SCAN... command, 78, 103

folders

scanning, 33

scanning automatically. *See* SafeZone, 94

selecting, 34

frequency

of scheduled scans, 53

of virus definitions updates, 54

G

general options, 77–78

GENERAL... command, 77, 105

H

halting scan, 79

halting the current operation, 40

hard disks. *See* disks

hardware required to run SAM, 17

help, 28–30

Help command button, 29

hot keys, 90–93

HOT KEYS... command, 90, 104

I

icon

Continue, 32

Delete, 33, 41

Details, 33, 46

display at startup, 77

Done, 33

Padlock, 97

icon (*continued*)

- Pause, 32
- Preferences, 24
- Print, 33, 37
- Repair, 33, 42
- selecting, 32
- Startup, 77
- Stop, 32

infected files

- allowing to run, 85
- defined, 24
- deleting, 41–42
- removing virus from, 40–43
- repairing, 42
- report, 40, 112

INIT conflicts, resolving, 117

inoculation discrepancy. *See* file changed alertinoculation. *See* fingerprint of files

Install dialog box, 18

install icon, 18

Installer-aware option, 85

installing SAM, 17

- on a network, 133
- problems with, 115
- SAM Intercept, 21
- SAM Intercept Jr., 21
- scanning during, 18
- selected features, 19–21

Intercept Jr., 21

Internet

- scanning files from, 94
- virus definition updates via, 71

irregular files

- defined, 84
- resolving potential problems with, 44–46
- scanning for, 84

Kkey combinations. *See* hot keys

known virus

- defined, 24
- descriptions of, 64
- eliminating, 40–44

known virus (*continued*)

- scanning for, 84–85
- See also* unknown virus

Llimited scan. *See* Quick scan optionlocked disk. *See* write-protected disk

logs of scan results, 88

M

Macintosh file system modifications, 82

Main Window, 26

manual, conventions of, 15

media, removable. *See* removable media

menu commands, 15

password-protecting, 95–97

reference, 99–105

MENU SECURITY... command, 95, 105

Menu Security dialog box, 95

messages, custom, 87

modem

settings, 69

using to update virus definitions, 66–69

modifying. *See* customizing

multi-user installations, 133–136

N

network

AppleShare, 133

AppleTalk, 133

delays while monitoring for viruses, 134

emergency response plan, 134, 134–136

installation, 133

Novell, 136

TOPS, 133

using SAM on, 133–136

virus detected on a, 136

network drives, scheduling scans of, 53

new virus. *See* unknown virus

Norton AntiVirus for NetWare, 136

Norton AntiVirus NLM
 sending alerts to, 87
 Novell, using SAM on, 133

O

options. *See* customizing

P

Padlock icon, 97
 PAGE SETUP... command, 99
 password
 changing, 97
 establishing, 96
 forgetting, 116
 removing, 97
 PASTE command, 100
 Pause icon, 32
 Preferences icon, 24
 Preferences menu, 103
 preferences. *See* customizing
 preventing
 access to infected floppy disks, 79
 access to specific SAM features, 95–97
 SAM from loading at system startup, 78
 virus infections, 51
 viruses via Internet. *See* SafeZone, 94
 PREVENTION... command, 80, 104
 Prevention feature
 customizing, 80–83
 levels of, 81
 on a server, 134
 Print icon, 32, 36
 PRINT REPORT... command, 37, 99
 printing
 Exceptions List, 58
 scan reports, 37, 99
 Proceed command button, 40, 49
 program, infected. *See* infected application

Q

Quick scan option, 84
 QUIT command, 27, 100

R

Remember command button, 48, 87
 removable media
 preventing access to infected, 79
 repairing, 43–44
 scanning, 35
 scanning automatically, 80
 removing
 alert boxes from screen, 87
 password-protection, 97
 suspicious activities from Exceptions List, 57
 viruses from infected files, 40–43
 renaming an application, 57
 REPAIR & EJECT command, 43, 101
 REPAIR command, 101
 Repair command button, 42
 Repair icon, 32
 repairing
 contrasted to replacing file, 41
 infected file, 42–43
 replacing infected files with uninfected copies, 41
 Report options, 88
 REPORT... command, 88, 104
 reports
 customizing, 88
 printing, 37
 saving to a file, 37, 99
 types of, 88
 requirements to run SAM, 17
 Resource Manager modifications, 82
 resource virus definition, 73
 results. *See* scan results

S

SafeZone
 changing, 94
 setting up, 94
 SAFEZONE...command, 94
 SAM
 about, 23
 adding virus definitions to, 66–74

SAM (*continued*)

- exiting, 27, 100
- installing, 17
 - problems with, 115
- Intercept Jr., 21
- Main Window, 23
- multi-user installations, 133
- password-protection of selected features, 95–97
- SAM Intercept
 - automatic protection with, 23, 25
 - defining hot keys for, 90–92
 - displaying icon for, 77
 - installing, 21
 - loading into memory, 28
 - preventing from loading at system startup, 78
 - preventing from loading first, 116
 - problems loading, 115
 - suspending alerts during software installation, 85
 - turning off and on, 28, 105
 - virus alert box, 39
- SAM Intercept Jr., 21
- scanning for viruses, 31–35
- site licenses, 133
- starting, 26
- system requirements, 17
- using on a network, 133–136
- using to remove virus from file, 39–44
- SAM Administrator, 133
- SAM Main Window, 26
- SAM Report file, 99
- SAM User Definitions file, 63
 - See also* virus definitions files
- SAM Virus Clinic. *See* SAM
- SAM Virus Definitions file, 63
 - See also* virus definitions files
- SAVE REPORT AS... command, 37, 99
- SCAN & EJECT command, 35, 101
- SCAN & PROTECT command, 101
- SCAN... command, 83, 103

scan results

- customizing reports, 88
- erasing, 100
- logs of, 88
- printing, 37, 99
- report of infected files, 40, 112
- report of irregular files, 45
- saving to a file, 37, 99
- summary of, 33, 36
- window, 33

scanning

- automatically, 52–53, 78–80
- before installation, 18
- compressed files, 93
- customizing, 83–85
- disks, 31–33
 - multiple floppy disks, 35
- during installation process, 18
- files, 33
 - downloaded, automatically, 94
- floppy disks, 35
 - automatically, 78–80
- folders, 33
- for file irregularities, 84
- for known viruses, 84–85
- for unknown viruses, 84
- halting while in progress, 79
- network disks, 133
- removable media, 35
- rental computers, 136
- scheduling, 52–53
- startup disk at installation, 18
- system folder, 53
- using hot keys, 90–92

SCHEDULER... command, 52, 102

Scheduler dialog box, 52

scheduling

- shutdown scans, 53
- startup scans, 53
- virus definitions updates, 54
- virus scans, 52–53

security. *See* password

SELECT ALL command, 34, 100

selecting

- all items in a list, 100
- by icon, 32
- by name, 34
- disks to scan, 32
 - all disks, 100
- features to install, 19–21
- files to scan, 34
- folders to scan, 34
- suspicious activities to monitor, 81–83

server. *See* file server

Set Preferences dialog box

- Alert options, 86
- Compression options, 93
- Floppy Scan options, 79
- General options, 77
- Hot Keys options, 90
- Prevention options, 80
- Report options, 88
- SafeZone, 94
- Scan options, 84

shutdown scans, scheduling, 53

site licenses, 133

SNIM. *See* SAM Administrator

software required to run SAM, 17

sound, warning, 87

SpaceSaver files, 93

Standard prevention level, 81

starting SAM, 26

startup disk

- checking for viruses at installation, 18
- scanning, 53

Startup Disk Builder, 59

Startup icon, 77

startup scans, scheduling, 53

startup, customizing, 77–78

Stop command button, 40

stopping in-progress floppy disk scan, 79

Stuffit files, 93

summary of scan, 32, 36

suspicious activity alerts, 47, 56

- determining presence of actual virus, 47
- displaying Remember button, 87

suspicious activity alerts (*continued*)

- Exceptions List of, 57–59
- monitoring for, 56–57, 80–83
- responding to, 47–48

Symantec AnitVirus for Macintosh. *See* SAM

Symantec BBS, 71

Symantec Network Installer for Macintosh. *See* SAM Administrator

system folder, scanning for viruses, 53

system messages, 121–132

system requirements to run SAM, 17

T

tape drives. *See* removable media

Tools menu, 101

TOPS, 133

transferring virus definitions

- from BBS, 70
- from Symantec, 67
- to another computer, 76
- to diskette, 76

Trojan horse, 41, 109

troubleshooting, 115

TURN INTERCEPT OFF command, 105

U

UNDO command, 100

unknown virus

- defined, 24, 56
- eliminating, 41
- indication for, 81–83
- protecting files from, 56–57
- scanning for, 84

See also known virus

update disk, 71

UPDATE VIRUS DEFINITIONS... command, 66, 102

Update Virus Definitions dialog box, 66

updating virus definitions

- automatically, 66–69
- frequency of, 54
- from BBS, 70
- from disk, 71

updating virus definitions (*continued*)

manually, 72–74

scheduling, 54

User definitions file, 63

V

virus

about, 107–109

alerts, 39–40

avoidance techniques, 51

defined, 24

definitions. *See* virus definitions

descriptions of, 64

detected on network, 136

differentiating from suspicious activity, 47

eliminating, 39–44

found during installation, 19

infection, 25

known, defined, 24

names, viewing list of, 64

newly discovered, 63

presence of, 39, 47

preventing, 51, 134

via Internet, 94

protecting against, 23, 25

protecting networks against, 135

removing from file, 40–44

response to in network environment, 134

scanning for, 31–35

spread of, 25

unknown

defined, 24, 56

indication for, 81–83

preventing, 81–83

protecting files from, 56–57

scanning for, 84

Virus Clinic file. *See* SAM Report file

Virus Clinic. *See* SAM

virus definitions

adding manually, 72–74

built-in, 63

copying to diskette, 76

data definition, 74

virus definitions (*continued*)

deleting, 75

downloading, 66–69

editing, 102

files, 63

resource definition, 73

updating

automatically, 66–69

frequency of, 54

from BBS, 70

from disk, 71

manually, 72–74

methods, 66

scheduling, 54

Virus Definitions dialog box, 64

virus definitions files

date of, 64

location of, 116

SAM cannot find, 116

types of, 63

updating, 66–74

virus scans

adding, 52–53

deleting, 55

editing, 55

scanning downloaded files, 94

scheduling, 52–53

volumes. *See* disks

W

warning

beep, 87

symbol for, 15

workstation

use of SAM on, 133–136

virus prevention on, 134

Worm, 109

write-protected disk

making, 143

virus infections on, 108